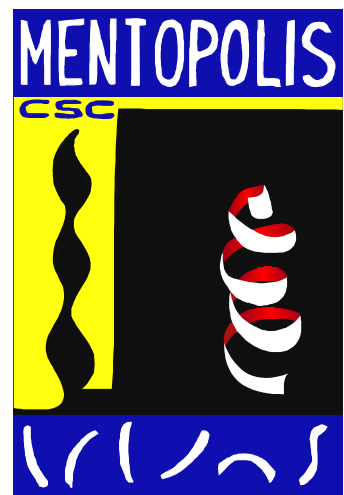


# Informationssicherheit im Application Service Providing (ASP)

- Whitepaper -

Mentopolis  
Consulting & Software Concepts GmbH

---



## Inhalt

<b>1</b>	<b><i>Sicherer ASP-Betrieb als Out-Sourcer</i></b>	<b>1</b>
<b>2</b>	<b><i>Informationssicherheits-Management</i></b>	<b>2</b>
<b>3</b>	<b><i>Datenschutz und Authentifizierung</i></b>	<b>3</b>
3.1	Datenhaltung .....	3
3.2	Session- und Transportsicherung .....	3
3.3	Authentifizierung durch Einmalpasswort .....	3

# 1 Sicherer ASP-Betrieb als Out-Sourcer

Naturgemäß wirft der Betrieb von Internet-basierten Anwendungen besondere Fragen bezüglich der Sicherheit der Kundendaten auf, insbesondere wenn es sich dabei um Anwendungen im Finanzbereich handelt, die im Kundenauftrag betrieben werden.

Kann „im Internet“ überhaupt Sicherheit hergestellt werden?

Kurz: ja, es kann. Es sind allerdings auch spezielle Anstrengungen zu unternehmen. Die Infrastrukturen und Dienstleistungen sind so zu konfigurieren und zu organisieren, dass Angriffe, Fehlfunktionen und Naturkatastrophen nach menschlichem Ermessen wirkungslos bleiben. Sollte sich dennoch etwas ereignen, muss der Schaden begrenzt und umgehend wieder Handlungsfähigkeit erreicht werden. Der überwiegende Teil möglicher Maßnahmen wird in den einschlägigen Standards bereits vorgeschlagen. Es bleibt die Umsetzung zu steuern, der Betrieb zu überwachen, die Entwicklung neuer Bedrohungen zu beobachten und gegebenenfalls neu auftauchenden Bedrohungen zeitnah mit angepassten Maßnahmen zu begegnen.

Mentopolis hat für diese Aufgabe ein Informations-Sicherheits-Management-System implementiert, das intern für die Kontrolle der Einhaltung aller Sicherheitsanforderungen sorgt. In dieses System binden wir externe, von uns beauftragte Dienstleister im erforderlichen Umfang ein. Im Abschnitt 2 beschreiben wir dieses Informationssicherheits-Management.

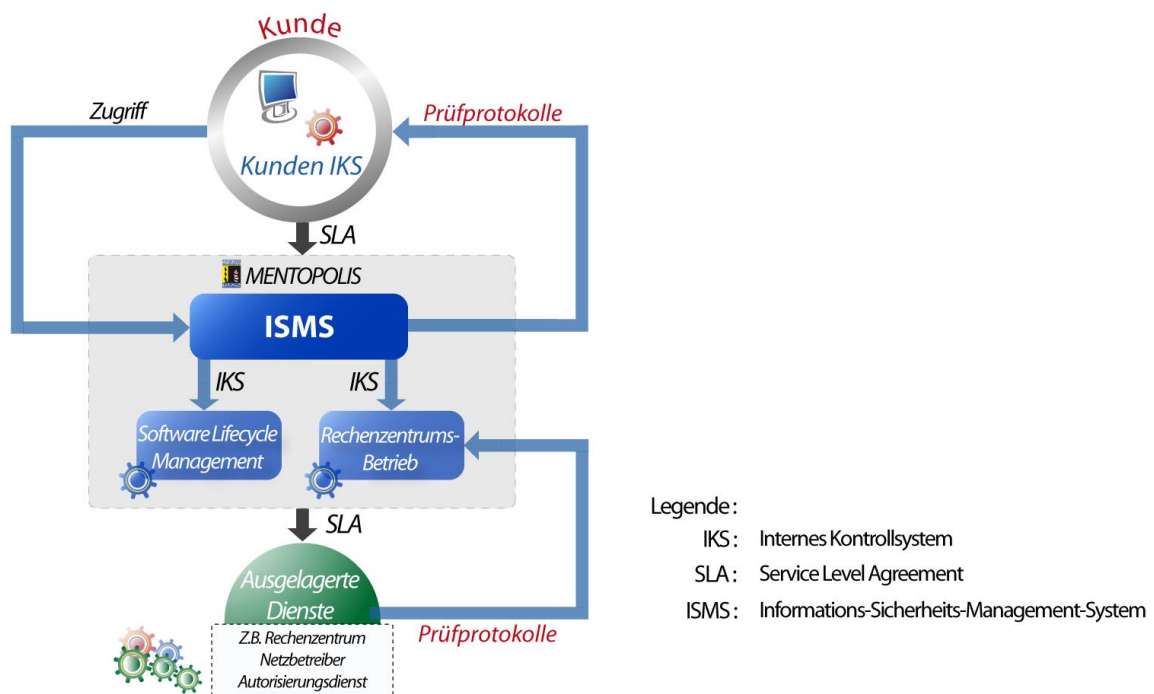
Die drei Informationssicherheits-Ziele Vertraulichkeit, Verfügbarkeit und Integrität werden durch geeignete Maßnahmen sichergestellt, die unter 3 umrissen werden. Für die Gewährleistung einer sicheren Authentifizierung von Nutzern der Webdienste wird ein besonderer Aufwand betrieben, der auf Basis eines Einmalpasswort-Generators den höchsten verfügbaren Sicherheitsstandard darstellt.

## 2 Informationssicherheits-Management

Die durch Mentopolis zur Verfügung gestellte Infrastruktur unterliegt einem Sicherheitsmanagement, das sich an den Vorgaben der Industriestandards orientiert (IT Grundschutz des BSI, ISO 17799). Die besonderen Anforderungen des Finanzwesens sind darüber hinaus zuletzt im Rundschreiben 18/2005 (MaRisk) der BaFin definiert worden, mit dem Ziel, bis 2007 verbindlich umgesetzt zu werden. Zum Management des operationellen Risikos wird dort der §25a Abs.2 KWG referenziert, dessen Bestimmungen deshalb die Basis für das vertragliche Angebot von Mentopolis an ihre sicherheitsbewussten Kunden aus dem Finanzwesen darstellen.

Mentopolis verfügt über ein eigenes internes Kontrollsystem zur Aufrechterhaltung des erforderlichen hohen Sicherheitsniveaus. Die Strukturen und Dokumente dieses IKS stehen unseren Kunden im vertraglich vereinbarten Umfang zur Verfügung (SLA).

Soweit Teildienstleistungen an weitere Anbieter ausgelagert werden müssen, werden an diese die gleichen Anforderungen gestellt. Unseren Kunden ist damit eine vollständige Kontrolle und ein den aktuellen Standards sowie den gesetzlichen Anforderungen entsprechendes eigenes Informationssicherheits-Management ermöglicht.



Weitere Details zum vereinbarten Umfang der Bewältigung des operationellen Risikos werden wie üblich in Service Level Agreements niedergelegt. Unser Kunde bestimmt dabei den Grad der gewünschten Sicherheit.

## 3 Datenschutz und Authentifizierung

Eine ASP-Anwendung, die sensible Kundendaten über das zunächst unsichere Internet transportiert, muss auf besondere Weise Zugang und Transportwege sowie Datenhaltung absichern. Diese Anforderung unterstützt Mentopolis durch eine Reihe von Maßnahmen entsprechend Industriestandard auf mehreren Ebenen.

### 3.1 Datenhaltung

- Die Datenbank, welche die Kundendaten aufnimmt, ist mandantenfähig. Kundendaten werden durch ein Berechtigungskonzept voneinander isoliert. Jeder Nutzer kann ausschließlich auf die Daten zugreifen, für die er autorisiert ist.
- Die physikalischen Server, welche die Datenbank enthalten, sind auf eine den gültigen Standards entsprechende Weise vor dem direkten Zugriff durch Unbefugte gesichert. Das schließt bewachte Räumlichkeiten mit Zugangskontrolle ein.
- Die Server werden mit Hilfe üblicher technischer und organisatorischer Maßnahmen im Rahmen des Möglichen vor Ausfall geschützt: weitgehend redundanter Aufbau, Redundanz in der Spannungsversorgung, Notstromaggregat, Datenspiegelung.
- Es werden geeignete Maßnahmen zum schnellen Wiederanlauf im Störfall ergriffen, wie z.B. redundante Datenhaltung und Sicherung des Datenbestands.

Details, die vor allem die Verfügbarkeit betreffen, werden flexibel nach Kundenanforderung in den SLA festgelegt.

### 3.2 Session- und Transportsicherung

Alle Wege, die vom ASP-System angeforderte oder gelieferte Daten über öffentliche Netze nehmen, werden auf Basis eines aktuell als sicher geltenden Verschlüsselungsverfahrens gesichert (SSL ab Version 3).

- Es wird eine Public Key-Infrastruktur zugrunde gelegt, deren Betreiber von der Bundesnetzagentur gemäß den Richtlinien des Signaturgesetzes zertifiziert ist.
- Die involvierten Server verfügen über hochsichere SSL-Zertifikate mit 128 Bit Schlüssellänge.
- Zu Beginn einer Session wird ein Session-Key ausgehandelt. Nach 10 Minuten ohne Aktivität wird die Session automatisch geschlossen.

### 3.3 Authentifizierung durch Einmalpasswort

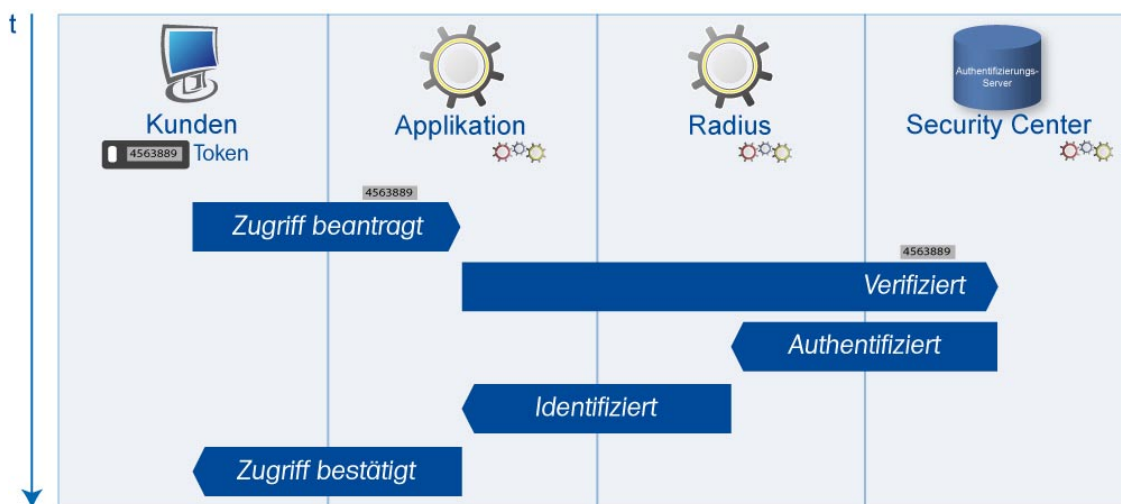
Ein Benutzer (Kunde), der über das öffentliche Netz auf den ASP-Dienst zugreift, muss sich mit Hilfe eines Hardware-Tokens authentifizieren. Das Hardware-Token ist ein kleines, etwa USB-Stick-großes Gerät, auf dem ein *Einmalpasswort* generiert wird, mit dem sich der Benutzer vor dem ASP-Dienst ausweist. Dieses Verfahren schützt vor dem Missbrauch ausgespähter Passwörter, da jedes Passwort immer nur für eine An-

meldung innerhalb eines kleinen Zeitfensters benutzt werden kann. Der Zugang zum Hardware-Token ist zusätzlich PIN-Code-geschützt.

Die eigentliche Validierung des Einmalpassworts erfolgt bei einem gesonderten, zertifizierten Provider, z.B. dem *Telekom Trust Center* (T-Systems) oder *Verisign*. Der Anwender am entfernten Rechner sieht eine Anmeldemaske zur ASP-Anwendung im Produkt-Lay-Out des Anbieters (also des Beauftragenden), die Anmeldenamen und Passwort abfragt. Der Anwender trägt die geforderten Informationen ein, wobei er als Passwort das von seinem Hardware-Token generierte Passwort benutzt. Diese Daten werden verschlüsselt an den Authentifizierungsserver übertragen, der sie validiert und im positiven Fall eine Nachricht, ebenfalls auf verschlüsseltem Wege, an den RADIUS\*-Server sendet.

Dieser prüft die dem nunmehr gesichert authentifizierten Benutzer zugehörigen Autorisierungen, also seine Zugriffsrechte auf dem Applikationsserver. Damit erhält der gesichert identifizierte Benutzer den gewünschten Zugriff, gemäß seinen vom Berechtigungskonzept der Anwendung gewährten Berechtigungen.

Die folgende Abbildung veranschaulicht das Prinzip:



\* "RADIUS" = **Remote Authentication Dial-In User Service**, ein Client-Server-Protokoll, das zur Authentifizierung, Autorisierung und zum Accountig von Benutzern in Computernetzen dient. Es ist der de facto-Standard bei zentraler Authentifizierung. Ursprünglich für Dial-In gedacht, wird RADIUS heute für die Zugangsverwaltung jeder Art von Fernzugriff genutzt (RFC 2865-2869).