Dokumentation Sicherheitsarchitektur

**01\_Technischer Basisschutz von IT-NT-Systemen**

Systemhärtung:

Req1: Nicht benötigte Dienste und Protokolle müssen deaktiviert werden.  
Req2: Die Erreichbarkeit von Diensten muss eingeschränkt werden.  
Req3: Nicht benötigte Software darf nicht installiert oder muss deinstalliert werden.  
Req4: Nicht benötigte Funktionen der eingesetzten Software und Hardware müssen deaktiviert  
 werden.

Systemaktualisierung

Req5: Software- und Hardware-Komponenten, für die es keine Wartung oder Pflege durch den   
 Lieferanten, Hersteller oder Entwickler gibt, dürfen nicht verwendet werden.  
Req6: Bekannt gewordene Schwachstellen in der Software oder Hardware des Systems müssen  
 behoben oder abgesichert werden.

Schutz von Daten und Informationen

Req7: Schutzbedürftige Daten müssen bei der Übertragung sowie Speicherung gegen unberechtigte  
 Einsichtnahme und Veränderung geschützt werden.  
Req8: Schutzbedürftige Informationen dürfen nicht in Dateien, Ausgaben und Meldungen enthalten  
 sein, die unautorisierten Benutzern zugänglich sind.

Schutz der Verfügbarkeit und Integrität

Req9: Das System muss sich gegen Überlastsituationen schützen.  
Req10: Falls eine Überlastsituation nicht verhindert werden kann muss sich das System berechenbar  
 verhalten  
Req11: Das System muss robust gegen unerwartete Eingaben sein.

Authentifizierung und Autorisierung

Req12: Die Nutzung und der Zugriff auf schutzbedürftige Funktionen und Informationen, dürfen  
 nicht ohne erfolgreiche Authentifizierung und Autorisierung möglich sein.  
Req13: Es müssen Konten verwendet werden, die die eindeutige Identifizierung des Benutzers  
 ermöglichen.   
Req14: Konten müssen gegen unautorisierte Nutzung durch Verwendung mindestens eines  
 Authentisierungsmerkmals geschützt werden.  
Req15: Konten mit weitereichenden Berechtigungen müssen mit zwei Authentisierungsmerkmalen   
 geschützt werden  
Req16: Vordefinierte Konten müssen gelöscht oder deaktiviert werden.  
Req17: Vordefinierte Authentisierungsmerkmale müssen geändert werden.  
Req18: Die Berechtigungen von Konten und Anwendungen müssen auf ein für deren Aufgaben  
 notwendiges Minimum reduziert werden.  
Req19: Das System muss für die Benutzerverwaltung an ein zentrales System angebunden werden.

Schutz von Sitzungen

Req20: Sitzungen müssen gegen eine unautorisierte Übernahme geschützt werden.  
Req21: Das System muss Benutzern ermöglichen sich von ihrer Sitzung abzumelden.  
Req22: Sitzungen müssen nach einer, dem Verwendungszweck angepassten Zeit der Inaktivität,  
 beendet werden.

Authentisierungsmerkmal Passwort

Req23: Falls Passwörter als Authentisierungsmerkmal genutzt werden, müssen diese mindestens 8  
 Zeichen lang sein und drei folgenden Zeichentypen beinhalten: Kleinbuchstaben,  
 Großbuchstaben, Ziffern und Sonderzeichen.  
Req24: Falls Passwörter als Authentisierungsmerkmal genutzt werden, muss eine Änderung des  
 eigenen Passwortes jederzeit durch den Benutzer möglich sein.  
Req25: Falls Passwörter als Authentisierungsmerkmal genutzt werden, muss ein Schutz gegen  
 Wörterbuch- und Brute-Force-Angriffe vorhanden sein, der das Erraten von Passwörtern  
 stark erschwert.  
Req26: Falls Passwörter als Authentisierungsmerkmal genutzt werden, darf deren Darstellung nicht  
 im Klartext erfolgen.

Protokollierung

Req27: Sicherheitsrelevante Ereignisse müssen abhängig vom Verwendungszweck des Systems mit  
 genauem Zeitstempel und einer eindeutigen Systembezeichnung protokolliert werden.  
Req28: Sicherheitsrelevante Protokollierungsdaten müssen umgehend nach deren Erzeugung an ein  
 separates System weitergeleitet werden.

**02\_Werb Services**

Allgemeine Vorgaben

Req1: Grundlegende Sicherheitsfunktionen für extern zugänglich Webservices müssen in der DMZ  
 implementiert werden und je nach Kritikalität mit einem Web Service Security Gateway  
 geschützt werden.  
Req2: Werden bei einem Webservice hochvertrauliche Daten im Sinne des Kreditkarten Payment  
 Standards PCI DSS (z.B. Kreditkartendaten, Kundendaten und Kundenpasswörter) verarbeitet,  
 so müssen diese Daten durch Einsatz von durchgängigen Mechanismen auf der  
 Anwendungsebene (End-to-End), wie z.B. XML-Verschlüsselung, individuell geschützt  
 werden.  
Req3: Ein Webservice-Requests muss vor Manipulation / Replay Attacken geschützt werden, wenn  
 dieser über öffentliche, ungesicherte Transportwege übertragen wird.

Authentifizierung

Req4: Der Absender eines Webservice-Requests muss angemessen authentifiziert werden, wenn  
 vertraulichen Inhalte / Informationen übertragen werden.  
Req5: Der Mechanismus zur Authentifizierung eines Absenders muss auf starken kryptografischen  
 Algorithmen / Frameworks basieren.  
Req6: Der Empfänger eines Webservice-Requests muss vom Absender dieses Request  
 authentifiziert werden.  
Req7: Wird ein Webservice-Request mit XML-Signaturen geschützt, dürfen die Signaturdaten NICHT  
 von einem Intermediate Processor aus dem Request entfernt werden.

SOAP und XML

Req8: Wenn ein SOAP-Request bzw. eine SOAP-Antwort nicht sofort abgewickelt wird und in der  
 DMZ zwischengespeichert werden muss, muss die Vertraulichkeit und Integrität der  
 zwischengespeicherten Nachricht sichergestellt werden.   
Req9: Ein neu entwickelter Webservice muss für die Inhalts-Formatvalidierung zwingend   
 XML-Schemata verwenden

WSDL

Req10: Jeder in einem Webservice vermittelte Element- und Attributwert muss mit dem erwarteten  
 Datentyp, der erwarteten Länge und/oder dem erwarteten Bereich beschrieben werden  
 sowie ggf. mit einer formellen Spezifikation zur Beschreibung der akzeptablen Daten.  
Req11: Alle Webservice-Requests MÜSSEN am Webservice-Endpunkt gegenüber der detaillierten  
 WSDL-Spezifikation validiert werden, die diesen Request beschreibt.  
Req12: Enthält der Webservice keine formelle Spezifikation der Eingabedaten, MUSS mittels Black-  
 /Whitelistings verhindert werden, dass illegale Zeichen an den Webserver weitergeleitet  
 werden.  
Req13: Der Öffentlichkeit darf nur die kleinstmögliche Anzahl an APIs / Funktionen über Webservices  
 zugänglich gemacht werden.

**03\_Webserver**

Plattformanforderungen

Req1: Der Webserver muss der einzige extern zugreifbare Service eines Systems sein, soweit der  
 Webserver nicht ausschließlich für eine Administrations-Schnittstelle genutzt wird.

Installationsanforderungen

Req2: Verschiedene Instanzen des Webservers müssen in getrennten Umgebungen laufen.  
Req3: Alle Webserverprozesse dürfen nicht mit Systemprivilegien laufen.

Konfigurationsanforderungen

Req4: Nicht benötigte http-Methoden müssen deaktiviert werden.  
Req5: Komponenten des Webservers, die für den Betrieb oder die Funktion nicht benötigt werden,  
 müssen deinstalliert werden.  
Req6: Falls CGI verwendet wird, müssen CGI-Wrapper für die erste Parameterüberprüfung/  
 -validierung und Einrichtung der korrekten Runtime- Umgebung für CGI-Programme  
 verwendet werden.  
Req7: Falls CGI verwendet wird darf das CGI-Verzeichnis keine Compiler oder Interpreter (bspw.  
 PERL-Interpreter, PHP-Interpreter/Compiler, TcI-Interpreter/Compiler oder Betriebssystem  
 Shells) enthalten.  
Req8: Falls CGI verwendet wird, darf das CGI-Verzeichnis nicht für Uploads genutzt werden.  
Req9: Falls Server Side Includes (SSI) aktiv sind, muss die Ausführung von Systembefehlen  
 deaktiviert werden.  
Req10: Falls WebDAV für das Schreiben von Dateien verwendet wird, darf Zugriff nicht ohne  
 erfolgreiche Authentifizierung gewährt werden.  
Req11: Falls WebDAV verwendet wird, müssen Zugriffsrechte restriktiv konfiguriert werden.  
Req12: Zugriffsrechte für Webserver-Konfigurationsdateien dürfen nur dem Eigentümer des  
 Webserver-Prozesses oder einem Benutzer mit Systemprivilegien gewährt werden.  
Req13: Default-Inhalte müssen entfernt werden.  
Req14: Schreibzugriff auf ausführbare Dateien, die mit Systemprivilegien ausgeführt werden, muss  
 auf Benutzer mit Systemprivilegien beschränkt werden.  
Req15: Die Erstellung von Verzeichnislisten (Indizierung) muss deaktiviert werden.  
Req16: Informationen über den Webserver in http-Headern müssen auf ein Mindestmaß beschränkt  
 werden.  
Req17: Informationen über den Webserver in Fehlerseiten, die durch den Webserver ausgeliefert  
 werden, müssen entfernt werden.  
Req18: Nicht benötigte Dateitypzuordnungen müssen entfernt werden.  
Req19: Das unautorisierte Überschreiben der Webserver-Konfiguration muss verhindert werden.  
Req20: Der Webserver darf nur Dateien ausliefern, die für die Auslieferung bestimmt sind.

HTTPS-Anforderungen

Req21: Für die Verschlüsselung mit HTTPS muss das TLS-Protokoll verwendet werden.  
Req22: Der Webserver muss so konfiguriert werden, dass die Nutzung der aktuellen Version des TLS  
 Protokolls möglich ist.  
Req23: Die TLS-Konfiguration darf keine unsicheren Cipher-Suites verwenden.  
Req24: Die TLS-Konfiguration muss vorsehen, dass beim Verbindungsaufbau die als am sichersten  
 einzustufenden Cipher-Suites mit oberster Priorität ausgewählt werden.

Protokollierung

Req25: Der Zugriff auf den Webserver muss protokolliert werden.

**04\_Secure Shell**

Sicherheitsanforderungen: Grundlegendes

Req1: Es muss ausschließlich die Protokollversion SSH-2 eingesetzt werden.  
Req2: Der SSH Dienst muss nicht benötigte Transport-Verschlüsselungsverfahren deaktivieren und  
 darf nur ein Verschlüsselungsverfahren oder minimale Auswahl von  
 Verschlüsselungsverfahren aus folgender Liste anbieten: AES128-CTR, AES192-CTR, AES256  
 CTR und [chacha20-poly1305@openssh.com](mailto:chacha20-poly1305@openssh.com)  
Req3: Der SSH-Serverdienst muss ausschließlich an die Schnittstellen und/oder IP-Adressen  
 gebunden werden, auf denen dieser Dienst erforderlich ist.  
Req4: Der SSH-Serverdienst muss als Stand-Alone Daemon ausgeführt werden.  
Req5: Als SSH-Server-Software muss OpenSSH zum Einsatz kommen.  
Req6: TCP/IP-Port-Weiterleitungen („Port Forwarding“) müssen kontrolliert eingesetzt werden.

SSH Optionen

Req7: Gateway-Ports dürfen nicht aktiviert werden.  
Req8: X11-Weiterleitungen müssen kontrolliert eingesetzt werden („X11-Forwarding“).  
Req9: SSH-„Agent Forwarding“ muss serverseitig deaktiviert werden.  
Req10: Tunnel Devices dürfen nicht benutzt werden („tunnel device forwarding“).  
Req11: Die Nutzung des SSH-Dienstes muss auf Gruppen (bzw. Benutzer) beschränkt werden.  
Req12: SSH-Logins müssen aufgezeichnet werden.

Authentifizierung und Accounts

Req13: Die Authentifizierung an Server-Systemen muss mittels asymmetrischer Kryptoverfahren  
 (Publickey, OTP) erfolgen.  
Req14: Eine Passwort-Authentifizierung (Passwortabfrage) darf nicht durch den SSH-Dienst  
 angeboten werden.  
Req15: Die Authentifizierungsinformationen der SSH-Benutzer (öffentliche SSH-Schlüssel im  
 Authorized-KeysFile) müssen kontrolliert und geschützt werden.  
Req16: Die vom SSH-Server zur Verfügung gestellten Funktionen und Dienste eines Users müssen auf  
 das erforderliche Minimum reduziert werden („Least Privilege“).  
Req17: Hot-basierte Authentifizierung (via rhosts/shosts) darf nicht verwendet werden.  
Req18: Der Fingerprint des Hostkeys oder der Hostkey muss zur Verfügung gestellt werden.  
Req19: Für SSH-Clients gilt, der Schlüssel des SSH-Servers (Hostkey) muss bei der Anmeldung  
 überprüft werden.

Anforderung für SSH-Clients

Req20: Für SSH-Client gilt, dass private Schlüssel geschützt werden müssen.  
Req21: Für SSH-Clients gilt, dass die Verwendung eines SSH-Authentifizierungsagenten (auf  
 Benutzer-Workstations/Terminals) durch eine Tastaturinteraktion kontrolliert freigegeben  
 werden muss. Ansonsten muss der Client den Authentifizierungsagenten nicht weiterleiten.  
Req22: Für SSH-Clients gilt, dass Gateway-Ports nicht auf Client-Seite aktiviert werden dürfen.

06\_Web-Anwendungen

Schutz von Daten und Informationen

Req1: Für Web-Anwendungen mit authentifizierten Sessions muss TLS mit Server-Authentisierung  
 und Verschlüsselung verwendet werden.  
Req2: Falls TLS eingesetzt wird, müssen alle Bestandteile der Web-Anwendung verschlüsselt  
 übertragen werden.  
Req3: Das Zertifikat der Web-Anwendung muss von einer Zertifizierungsstelle ausgestellt werden,  
 deren Zertifikate von den gängigen Browsern der Benutzer der Web-Anwendung erkannt  
 werden.  
Req4: Das Zertifikat der Web-Anwendung muss spätestens nach 36 Monaten seine Gültigkeit  
 verlieren.  
Req5: Das Zertifikat der Web-Anwendung muss eine Schlüssellänge von mindestens 2048 Bit  
 aufweisen (bei Verwendung von RSA).  
Req6: Um schutzbedürftige Daten zu übertragen, darf die Web-Anwendung keine URL-Parameter  
 verwenden.  
Req7: Die Web-Anwendung darf clientseitig keine schutzbedürftige Informationen speicher, weder  
 temporär noch persistent. Dies gilt sowohl für Cookies als auch für andere Arten von lokalen  
 Speichern des Browsers.  
Req8: Die Web-Anwendung muss verhindern, dass schutzbedürftige Daten, die der Benutzer in ein  
 HTML-Formular eingibt, vom Browser gespeichert und bei der nächsten Verwendung  
 automatisch vervollständigt werden. Hierzu muss die Web-Anwendung das Attribut  
 „autocomplete = „off““ setzen.  
Req9: Die Web-Anwendung muss das Caching schutzbedürftige Daten verhindern.  
Req10: Die Web-Anwendung muss den Zugriff von externen Suchmaschinen und von internen  
 Suchfunktionen auf die Dateien und Inhalte einschränken, die angezeigt werden dürfen.

Schutz der Verfügbarkeit und Integrität

Req11: Die Web-Anwendung muss sämtliche Daten, die von einem Client übertragen werden,  
 serverseitig validieren.  
Req12: Falls Eingabedaten bereits von einer clientseitigen Logik der Web-Anwendung verarbeitet  
 werden, ohne dass die Möglichkeit besteht, dass sie vorher serverseitig validiert werden,  
 müssen die Daten vor der Verarbeitung clientseitig validiert werden.  
Req13: Sämtliche Daten, die von einem anderen System übertragen werden, müssen zunächst von  
 der Web-Anwendung als nicht vertrauenswürdig betrachtet werden. Abhängig von der  
 Kritikalität der Web-Anwendung und der Vertrauenswürdigkeit des anderen Systems muss  
 die Web-Anwendung auch diese Daten validieren.  
Req14: Die Eingabevalidierung der Web-Anwendung muss über Whitelisting erfolgen.  
Req15: Falls die Web-Anwendung bei der Validierung von Daten feststellt, dass die Daten von den  
 erwarteten Inhalten oder Formaten abweichen, muss die Web-Anwendung diese Daten  
 zurückweisen und die angeforderte Aktion abbrechen.  
Req16: Die Web-Anwendung darf keine Eingabedaten von Benutzern für den direkten Zugriff auf  
 Dateien oder auf andere serverseitige Ressourcen verwenden.  
Req17: Falls Dateien von einem Client hochgeladen oder von anderen Systemen übertragen werden  
 können, muss die Web-Anwendung diese Dateien überprüfen und so verarbeiten, dass keine  
 Gefährdungen für die Anwendung oder für Benutzer entstehen.  
Req18: Falls von der Web-Anwendung Daten an ein anderes System oder an einen Client (Browser)  
 übertragen werden, muss die Web-Anwendung gewährleisten, dass diese Daten dort keine  
 unerwünschten Aktionen auslösen bzw. keinen anderen unerwünschten Effekt haben.  
Req19: Jede Ausgabe der Web-Anwendung muss in einer korrekten und definierten Codierung sowie  
 mit Angabe des korrekten MIME-Types erfolgen.  
Req20: Die Web-Anwendung muss sämtliche Eingabedaten, die sie an den Brwoser zurücksendet,  
 validieren und dabei alle Metazeichen HTML-codieren, um Cross-Site-Scripting (XSS) zu  
 verhindern.  
Req21: Falls Textformatierungen in Benutzereingaben erlaubt sind, muss in der Web-Anwendung ein  
 Whitelist-Eingabefilter für unterstützte und zulässige HTML-Tags implementiert sein, um  
 Cross-Site-Scripting (XSS) zu verhindern.  
Req22: Falls für Benutzereingaben eine Markup-Sprache verwendet wird, die in HTML konvertiert  
 wird (z.B. BBCode), muss in der Web-Anwendung zusätzlich ein Whitelist-Eingabefilter für  
 zulässige Tags implementiert sein, um Cross-Site.Scripting (XSS) zu verhindern.  
Req23: Falls Änderungen am DOM (Document Object Model) einer Webseite möglich sind, die auf  
 manipulierbaren Eingabedaten basieren, müssen diese Eingabedaten auf dem Client  
 hinsichtlich Metazeichen validiert und entsprechend codiert werden, um DOM-basiertes  
 Cross-Sites-Scripting (XSS) zu verhindern.  
Req24: Falls die Web-Anwendung Eingabedaten außerhalb des HTML-Bodys ausgibt (also z.B. in der  
 URL, im JavaScript oder im CSS), muss die Ausgabe durch Escapen der Eingabedaten  
 abgesichert werden, um Cross-Site-Scripting (XSS) zu verhindern. Das Escapen muss abhängig  
 vom jeweiligen Kotext erfolgen.  
Req25: Falls Eingabedaten bei der Bildung von Datenbank-Abfragen verwendet werden, muss die  
 Web-Anwendung Interpreter-Injection (SQL-Injection bzw. NoSQL-Injection) durch geeignete  
 Gegenmaßnahmen verhindern.  
Req26: Falls die Web-Anwendung XML-Datenstrukturen, XSLT-Stylesheets oder XPath-Queries  
 erstellt und falls sie hierfür auch Eingabedaten der Benutzer verwendet, muss die Web  
 Anwendung XML-Injection bzw. XPath-Injection durch geeignete Gegenmaßnahmen  
 verhindern.  
Req27: Um Code- bzw. Command-Injection zu verhindern, darf die Web-Anwendung keine  
 Eingabedaten der Benutzer verwenden, um Shell-Befehle oder Befehle für das laufende  
 Programm (z.B. über eval()) zu erstellen. Dies gilt sowohl auf Serverseite als auch auf  
 Clientseite.  
Req28: Falls die Web-Anwendung Eingabedaten der Benutzer verwendet, um http-Header zu bilden,  
 müssen diese Daten ausreichend validiert werden: Gefährliche Zeichen, insbesondere CR und  
 LF (%0d und %0a), müssen gefiltert werden, bevor die Eingabedaten in die Header einer http  
 Response eingefügt werden.  
Req29: Die Web-Anwendung darf keine Eingabedaten von Benutzern verwenden, um daraus URLs  
 für Weiterleitungen (Redirects) zu bilden oder anderweitig URLs zu erstellen.  
Req30: Es muss verhindert werden, dass über die Web-Anwendungen E-Mail-Kommandos in einen  
 nachgelagerten Mail-Server injiziert werden (E-Mail-Injection).  
Req31: Falls es möglich ist, aus der Web-Anwendung heraus ohne vorherige Authentisierung E-Mails  
 oder SMS zu initiieren (z.B. bei einer Passwortrücksetzung oder für eine Weiterempfehlung)  
 oder Daten an die Web-Anwendung zu schicken (z.B. Kontaktformulare oder  
 Seitenbewertungen), muss die Web-Anwendung durch angemessene  
 Sicherheitsmechanismen Missbrauch dieser Funktionalitäten (insbesondere für SPAM oder  
 Denial-of-Service) verhindern.

Authentifizierung und Autorisierung

Req32: Die Web-Anwendung muss bei jeder Aktion eines Benutzers serverseitig verifizieren, dass  
 dieser Benutzer berechtigt ist, auf die Daten / Inhalte zuzugreifen bzw. die Funktion  
 auszuführen.  
Req33: Die Web-Anwendung muss den korrekten Transaktionsfluss serverseitig kontrollieren, um  
 sicherzustellen, dass die Anwendungslogik nicht umgangen werden kann.  
Req34: Falls die Web-Anwendung im Internet erreichbar ist, muss der Registrierungsprozess der  
 Web-Anwendung sicherstellen, dass Registrierungen nicht automatisiert durchgeführt  
 werden können.  
Req35: Die Web-Anwendung muss eine erneute Authentisierung des Benutzers verlangen, wenn der  
 Benutzer kritische Daten ändern oder kritische Aktionen auslösen will. Insbesondere muss  
 die Web-Anwendung bei einer Passwortänderung die erneute, korrekte Eingabe des  
 aktuellen Passworts (sowie die zweimalige Eingabe des neuen Passworts) verlangen.  
Req36: Falls für die Web-Anwendung ein Single-Sign-On Verfahren realisiert wird, das auf  
 Authentifizierungstickets basiert, müssen Replay-Angriffe sowie unrechtmäßige Verwendung  
 von Tickets verhindert werden.  
Req37: Falls die Web-Anwendung netzbasierte Authentisierung von mobilen Endgeräten über http  
 Header (z.B. x-forwarded-for) akzeptiert, muss sichergestellt sein, dass diese Header  
 Information von internen Systemen (z.B. MIG, Mobile Internet Gateway) kommt und nicht  
 manipuliert wurde.  
Req38: Falls die Web-Anwendung einem Benutzer Zugriff auf Kundendatensätze Dritter ermöglicht,  
 muss festgestellt werden, wenn ein definierter Schwellwert für Zugriffe auf  
 Kundendatensätze überschritten wird. In dem Fall müssen durch geeignete  
 Gegenmaßnahmen weitere Zugriffe verhindert werden.  
Req39: Falls die Web-Anwendung eine Suchfunktion für Kundendatensätze Dritter beinhaltet,  
 müssen die Suchoptionen so weit wie möglich eingeschränkt werden.  
Req40: Falls die Web-Anwendung eine Suchfunktion für Kundendatensätze Dritter beinhaltet,  
 muss die Anzahl der Suchergebnisse, die die Suchfunktion zurückliefert, begrenzt werden.  
Req41: Falls die Web-Anwendung eine Funktion für den Massenexport von Kundendatensätzen  
 Dritter vorsieht, muss diese Funktion auf individuelle und dokumentierte Benutzer  
 eingeschränkt werden. Zudem muss die Web-Anwendung protokollieren, wenn ein Benutzer  
 diese Exportfunktion nutzt.  
Req42: Falls die Web-Anwendung einem Benutzer Zugriff auf Kundendatensätze Dritter ermöglicht,  
 muss das Einverständnis des Kunden vor Aufruf bzw. Anzeige detaillierter Kundendaten  
 verifiziert werden.

Schutz von Sitzungen

Req43: Die Länge der Session-Identifier der Web-Anwendung muss mindestens 120 Bit betragen.  
Req44: Zur Übertragung des Session-Identifiers müssen Cookies verwendet werden („Session  
 Cookies“)  
Req45: Ein Session-Cookie darf nicht persistent sein.  
Req46: Falls die Session mittels TLS gesichert wird, muss die Web-Anwendung im Session-Cookie das  
 Attribut „secure“ setzen.  
Req47: Die Web-Anwendung muss im Session-Cookie das Attribut „httpOnly“ setzen.  
Req48: Die Web-Anwendung darf das Attribut „domain“ im Session-Cookie nicht setzen.  
Req49: Die Web-Anwendung muss das Attribut „path“ im Session-Cookie so restriktiv setzen, dass  
 der Cookie nicht an andere Web-Anwendungen auf dem gleichen Host gesendet wird.  
Req50: Nach erfolgreicher Authentifizierung eines Benutzers muss die Web-Anwendung einen neuen  
 Session-Identifier erzeugen und an den Browser des Benutzers senden.  
Req51: Für ein Benutzerkonto darf nur eine Session zur selben Zeit aktiv sein.  
Req52: Die Web-Anwendung muss über eine Funktion verfügen, die es dem angemeldeten Benutzer  
 ermöglicht, sich jederzeit abzumelden.  
Req53: Falls ein Benutzer über ein Single-Sign-On Verfahren Zugang zu der Web-Anwendung  
 erhalten hat und sich in der Web-Anwendung wieder abmeldet, müssen beide Sessions  
 beendet werden: sowohl die Session mit der Web-Anwendung als auch die Session mit dem  
 ursprünglichen SSO-Portal.  
Req54: Falls ein Benutzer über ein Single-Sign-On Verfahren Zugang zu der Web-Anwendung  
 erhalten hat und sich vom SSO-Portal abmeldet, muss auch die Session mit der Web  
 Anwendung automatisch beendet werden.  
Req55: Nach einer definierten Zeit der Inaktivität des Benutzers muss in der Web-Anwendung ein  
 Session-Timeout erfolgen.  
Req56: Bei einer Abmeldung oder einem Timeout muss die Web-Anwendung die Session und den  
 dazugehörigen Session-Identifier serverseitig ungültig machen.  
Req57: Die Web-Anwendung muss einen Mechanismus gegen Angriffe mittels Cross-Site-Request  
 Forgery (CSRF) einsetzen. Dieser Mechanismus muss verhindern, dass ein Angreifer  
 gefälschte Requests auf einer von ihm kontrollierten Webseite hinterlegen kann, die beim  
 Besuch dieser Webseite (durch angemeldete Benutzer der Web-Anwendung) automatisch  
 Aktionen in der Wen-Anwendung auslösen.  
Req58: Die Web-Anwendung muss einen Mechanismus gegen Clickjacking-Angriffe einsetzen, der  
 verhindert, dass die Web-Anwendung von anderen unberechtigten Web-Anwendungen  
 innerhalb eines IFrame dargestellt wird.  
Req59: Falls JSON für die Übertragung schutzbedürftiger Daten verwendet wird, muss die Web  
 Anwendung eine geeignete Maßnahme gegen JSON-Hijacking einsetzen.  
Req60: Berechtigung für Cross-Domain-Zugriffe auf die Web-Anwendung müssen restriktiv definiert  
 werden, d.h. ausschließlich für die Hosts, für die dies zwingend erforderlich ist.  
Req61: Cross-Domain-Zugriffe auf schutzbedürftige Inhalte der Web-Anwendung dürfen nicht  
 ermöglicht werden.  
Req62: Intranet-Anwendungen dürfen keine Berechtigungen für Cross-Domain-Zugriffe gewähren für  
 Domains, die nicht zum Intranet gehören.  
Req63: Nicht vertrauenswürdige Flash- oder Silverlight-Dateien, die von der Web-Anwendung  
 ausgeliefert werden, müssen in einer separaten Domain für nicht vertrauenswürdige Inhalte  
 platziert werden. Sie dürfen keine Berechtigungen für Cross-Domain-Zugriffe erhalten.  
Req64: Flash- oder Silverlight-Dateien, die von der Web-Anwendung ausgeliefert werden, dürfen  
 nicht auf externe, nicht vertrauenswürdige Daten zugreifen oder entsprechende Inhalte  
 laden.  
Req65: Die Web-Anwendung darf keine RIA-Services nutzen, die die „Same-Origin-Policy“ umgehen.

Authentisierungsmerkmal Passwort

Req66: Falls Passwörter als Authentisierungsmerkmal genutzt werden, muss der  
 Registrierungsprozess der Web-Anwendung sicherstellen, dass ein Benutzer sein Passwort  
 selber wählt. Entweder setzt der Benutzer das Passwort direkt bei der Registrierung; oder  
 erhält (z.B. per E-Mail) ein individuelles Initialpasswort, das er bei der ersten Anmeldung  
 sofort ändern muss.  
Req67: Falls für den Registrierungsprozess der Web-Anwendung Initialpasswörter (bzw.  
 Aktivierungstoken) verwendet werden, müssen diese nach einer angemessenen Zeit ihre  
 Gültigkeit verlieren.  
Req68: Falls Passwörter als Authentisierungsmerkmal genutzt werden, muss die Web-Anwendung  
 über einen gegen Missbrauch geschützten Prozess verfügen, über den der Benutzer sein  
 Passwort zurücksetzen lassen kann.  
Req69: Bei einem fehlgeschlagenen Anmeldeversuch eines Benutzers darf die Web-Anwendung  
 keine Information ausgeben, welche der eingegebenen Anmeldeinformationen nicht korrekt  
 war.

Content-Management-Systeme (CMS)

Req70: Der Zugang zur Redaktionsumgebung des Content Management Systems darf nicht aus dem  
 Internet erfolgen.  
Req71: Das Content Management System muss es ermöglichen, Berechtigungen für unterschiedliche  
 Tätigkeiten des Content-Managements verschiedenen Nutzern / Nutzergruppen zuzuweisen,  
 so dass ein mehrstufiger Veröffentlichungsprozess realisiert werden kann.  
Req72: Das Content Management System muss es ermöglichen, bestimmte Inhalte Exklusiv  
 bestimmten Redakteuren oder einer Gruppe von Redakteuren zuzuweisen.  
Req73: Falls das Content Management System Funktionen bereitstellt, um Inhalte zu erstellen, die  
 erst zu einem späteren Zeitpunkt veröffentlicht werden soll, dürfen diese Inhalte vorher in  
 der Web-Anwendung nicht einsehbar oder auffindbar sind.  
Req74: Das Content Management System muss Funktionen bereitstellen, die es erlauben, die  
 Verwendung von aktivem Content und Scripting innerhalb der erstellten Inhalte  
 einzuschränken (auf bestimmte Inhalte bzw. für besitmmte Benutzergruppen) und ggf. ganz  
 zu unterbinden.  
Req75: Preview-Funktionalitäten des Content Management Systems müssen vor unberechtigtem  
 Zugriff geschützt werden: Nur erfolgreich authentisierte Benutzer des CMS dürfen die Inhalte  
 des Previews einsehen; sie dürfen hierbei auch nur auf die Inhalte zugreifen, für die sie  
 mindestens Lese-Rechte haben.