		Funktionale Sicherheitsanforderungen	Mozilla Firefox 51.0.1	Google Chrome 56.0.2924.87	Microsoft Internet Explorer 11.103.14393.0	Microsoft Edge 38.14393.0.0
Kategorie	***ID***	***Beschreibung***				
Vertrauenswürdige Kommunikation	4.2.1.1	Das Protokoll TLS, Version 1.2 muss gem. Mindeststandard TLS 1.2 unterstützt werden.	ja	ja	ja	ja
	4.2.1.2	Der Web-Browser muss eine Liste von Zertifikaten vertrauenswürdiger Zertifikatsaussteller (CA-Zertifikat) bereitstellen. Der Web-Browser muss Zertifikate mit erweiterter Prüfung (Extended-Validation-Zertifikate) unterstützen. Der schreibende Zugriff auf den Zertifikatsspeicher darf nur mit administrativen Rechten oder mit der expliziten Zustimmung des Benutzers erfolgen. Insbesondere muss ein lokaler Widerruf von Zertifikaten möglich sein.	ja	ja	ja	ja
	4.2.1.3	Der Web-Browser muss eine vollständige Überprüfung der Gültigkeit des Serverzertifikats durchführen. Diese Prüfung betrifft neben dem Serverzertifikat alle weiteren CA-Zertifikate der Zertifikatskette bis zum Wurzelzertifikat. Die Überprüfung beinhaltet die mathematische Prüfung des Zertifikats mit Hilfe des öffentlichen Schlüssels des ausgestellten CA-Zertifikats sowie die Prüfung der zeitlichen Gültigkeit des Zertifikats und die Überprüfung des Sperrstatus des Zertifikats (CRL oder OCSP).	ja	ja	ja	ja
	4.2.1.4	Der Web-Browser muss die Kommunikationsform geeignet und nicht manipulierbar darstellen: Dem Benutzer muss beispielsweise durch Symbole oder farbliche Hervorhebung angezeigt werden, ob die Kommunikation mit dem Web-Server verschlüsselt oder im Klartext erfolgt. Es muss die Möglichkeit bestehen, im Falle einer verschlüsselten Kommunikation auf Anforderung des Benutzers das verwendete Serverzertifikat, die verwendete SSL/TLS-Protokollversion und Cipher-Suite anzeigen zulassen. Dem Benutzer muss ein fehlendes CA-Zertifikat im Zertifikatsspeicher oder ein ungültiges/widerrufenes Serverzertifikat als Prüfergebnis signalisiert werden.Die verschlüsselte Verbindung darf dann nur nach expliziter Bestätigung durch den Benutzer aufgebaut werden.	ja	ja	ja	nein Keine Anzeige von Protokollversion und Cipher Suite. Lösung: Seite über Optionsmenü mit IE anzeigen lassen.
	4.2.1.5	Der Web-Browser muss HSTS gem. RFC 6797 unterstützen.	ja	ja	ja	ja
Schutz des Webbrowsers	4.2.1.6	Software-Update-Mechanismen erfüllen folgende Anforderungen: Software-Update-Mechanismen müssen sämtliche Web-Browserkomponenten umfassen (inkl. Erweiterungen und Plug-ins). Eigenständige Programme, die zusätzlich Elemente in den Browser einfügen (z. B. EXE-Dateien für Internet Explorer, die Buttons einrichten), müssen über separate Update-Prozesse aktuell gehalten oder untersagt werden Software-Updates müssen erkannt werden. Software-Updates müssen zuverlässig angezeigt werden. Automatisches Einspielen von Updates muss möglich sein.	ja	ja	ja	ja
	4.2.1.7	Integritätsprüfungen der Updates erfüllen folgende Anforderungen: Updates dürfen nur dann eingespielt werden, wenn die Prüfung der Integrität ein positives Prüfergebnis liefert. Nicht korrekte Prüfergebnisse müssen dem Benutzer signalisiert werden. Das Update darf in diesem Fall nicht eingespielt werden.	ja	ja	ja	ja
Identifikation und Authentisierung	4.2.1.8	Sichere Passwortmanager erfüllen folgende Eigenschaften: Passwortmanager müssen eine eindeutige Zuordnung zwischen Webseite (URL) und hierfür gespeichertem Passwort zuverlässig ermöglichen. Passwörter müssen besonders geschützt abgespeichert werden (z. B. verschlüsselt). Diese Sicherheitsanforderungen sind nur dann anzuwenden, wenn Passwortmanager genutzt werden. Zur Umsetzung können auch externe Add-ons verwendet werden.	ja	ja	ja	ja
	4.2.1.9	Der Passwortmanager darf einen Zugriff auf gespeicherte Passwörter nur nach Eingabe eines Master-Passworts durch den Benutzer ermöglichen. Jede neue Browser-Sitzung muss eine erneute Authentisierung für den Zugriff auf gespeicherte Passwörter erfordern.	ja	eingeschränkt Lösung: Externe Erweiterung	eingeschränkt Lösung: Externe Erweiterung	eingeschränkt Lösung: Externe Erweiterung
	4.2.1.10	Bereits gespeicherte Passwörter und das Master-Passwort müssen auf Anforderung des Benutzers gelöscht werden können.	ja	ja	ja	ja
Schutz vertrauenswürdiger Daten	4.2.1.11	Das Anlegen von Cookies muss auf Anforderung des Benutzers deaktiviert werden können.	ja	ja	ja	ja
	4.2.1.12	Bereits angelegte Cookies müssen auf Anforderung des Benutzers gelöscht werden können.	ja	ja	ja	ja
	4.2.1.13	Die Nutzung von Drittanbieter-Cookies muss auf Anforderung des Benutzers blockiert werden können.	ja	ja	ja	ja
	4.2.1.14	Autofill-Funktionalitäten (Name, Email, usw.) müssen auf Anforderung des Benutzers deaktiviert werden können.	ja	ja	ja	ja
	4.2.1.15	Die Liste der besuchten Seiten (Historie) und die Autofill-Historien müssen auf Anforderung des Benutzers gelöscht werden können.	ja	ja	ja	ja

		Funktionale Sicherheitsanforderungen	Mozilla Firefox 51.0.1	Google Chrome 56.0.2924.87	Microsoft Internet Explorer 11.103.14393.0	Microsoft Edge 38.14393.0.0
Kategorie	***ID***	***Beschreibung***				
Überprüfung auf schädliche Inhalte	4.2.1.16	Adress- und inhaltsbasierte Schutzmechanismen (wie z. B. SafeBrowsing) sind implementiert.	ja	ja	ja	ja
	4.2.1.17	Adressbasierte Überprüfung: Liegen Informationen über schädliche Inhalte vor, muss der Benutzer beim Aufrufen der Webseite in geeigneter Form gewarnt werden. Die Überprüfung sollte vorrangig auf Basis lokal vorgehaltener Listen erfolgen. Eine als schädlich eingestufte Verbindung darf erst nach expliziter Bestätigung durch den Benutzer aufgebaut werden.	ja	ja	ja	ja
	4.2.1.18	Inhaltsbasierte Überprüfung: Vor eventuell schädlichem Inhalt (Dateien) wird der Benutzer entsprechend gewarnt.	ja	ja	ja	ja
Same-Orgin-Policy	4.2.1.19	Eine sinnvolle Same-Origin-Policy ist umzusetzen. Insbesondere dürfen Dokumente und Skripte (Client) nicht auf Ressourcen (z. B. Grafiken, Textfelder) anderer Web-Seiten zugreifen.	ja	ja	ja	ja
	4.2.1.20	Herkunft (Origin) einer Webseite muss als Kombination aus den Parametern „Protokoll“, „Domain“ und ggf. angegebenem „Port“ in der Adresse (URL) ausgewertet werden. Ein Zugriff auf Ressourcen ist ausschließlich erlaubt, wenn alle drei Parameter in der URL identisch sind.	ja	ja	ja	ja
Sichere Konfiguration	4.2.1.21	Sichere Konfiguration: Eine zentrale Oberfläche für die Verwaltung der Einstellungen muss bereitstehen. Einstellungen, um Plug-ins, Erweiterungen und JavaScript aktivieren und deaktivieren zu können, müssen vorhanden sein.	ja	ja	ja	ja
	4.2.1.22	Zentrale Verwaltung: Der Import von zentral erstellten Konfigurationen muss möglich sein.	ja	ja	ja	ja
	4.2.1.23	Synchronisation: Sofern vorhanden, muss eine Synchronisation mit externen Speicherdiensten und -orten (sog. Cloud-Dienste) deaktivierbar sein.	ja	ja	ja	ja
	4.2.1.24	Browser-Instanzen: Der Web-Browser muss parallel in unterschiedlich konfigurierten Browser-Instanzen betrieben werden können.	ja	eingeschränkt Lösung: Zweite Instanz via portabler Version	eingeschränkt Lösung: Zweiter Browser in anderer Konfiguration	eingeschränkt Lösung: Zweiter Browser in anderer Konfiguration
Minimale Rechte	4.2.1.25	Der Web-Browser muss nach seiner Initialisierung mit minimalen Rechten im Betriebssystem ablaufen. Die Managementkomponente (Ressourcenmanager) darf nicht dauerhaft die Rechte eines Administrators erfordern, um ablaufen zu können. Bei der Initialisierung kann der Web-Browser mit erweiterten Rechten laufen, diese sind danach aber wieder abzutreten. Lese- und Schreibzugriffe der Darstellungskomponenten sind ausschließlich auf festgelegte Bereiche des Dateisystems zulässig. Aufrufe von Betriebssystemfunktionen durch Darstellungskomponenten dürfen ausschließlich über wohldefinierte Schnittstellen der Ressourcenmanager erfolgen.	eingeschränkt Lösung: GPO-Add-on, sonstiger Workaround.	ja	ja	ja
Sandboxing und Kapselung	4.2.1.26	Der Web-Browser muss eine Architektur mit folgenden Eigenschaften bereitstellen: Sämtliche Komponenten müssen voneinander und zum Betriebssystem hin gekapselt sein. Direkter Zugriff auf Ressourcen isolierter Komponenten darf nicht möglich sein. Kommunikation zwischen den isolierten Komponenten darf nur über definierte und kontrollierte Schnittstellen erfolgen. Darstellungskomponenten für aktive Inhalte wie Flash und JavaScript sind gesondert gekapselt.	ja	ja	ja	ja
	4.2.1.27	Web-Seiten müssen voneinander isoliert werden, idealerweise in Form eigenständiger Prozesse. Eine Isolation auf Thread-Ebene ist aber ebenfalls zulässig.		ja	ja	ja
	4.2.1.28	Der Web-Browser muss die Content Security Policy mindestens in der Version 1.0 gem. den W3C-Spezifikationen umsetzen.	ja	ja	ja	ja

		Organisatorische Sicherheitsanforderungen	Mozilla Firefox 51.0.1	Google Chrome 56.0.2924.87	Microsoft Internet Explorer 11.103.14393.0	Microsoft Edge 38.14393.0.0
Kategorie	***ID***	***Beschreibung***				
Entwicklung	4.2.2.1	Es sind nur Programmiersprachen und -werkzeuge zulässig, die sichere Funktionen unterstützen und Mechanismen zum Stack- und Heapschutz implementieren. Der Web-Browser muss die vom Betriebssystem bereitgestellten Speicherschutzmechanismen nutzen können.	ja	ja	ja	ja
Aktualisierung	4.2.2.2	Nach Bekanntwerden einer kritischen Schwachstelle soll durch den Anbieter innerhalb von 21 Tagen ein Software-Update zur Verfügung gestellt werden. Die Auslieferung der Updates muss integritätsgesichert erfolgen. (Für Anforderungen bzgl. Aktualisierungen an den Betreiber siehe ID 4.3.6.)	ja	ja	ja	ja
Fehlerbehebung	4.2.2.3	Um potenzielle Schwachstellen melden zu können, müssen Kontaktmöglichkeiten zu Sicherheitsteams des Anbieters bereitgestellt werden.	ja	ja	ja	ja
Datensicherheit	4.2.2.4	Um Überprüfungen auf schädliche Inhalte (u. a. Pishing) durchführen zu können, müssen aktuelle Listen bereitgestellt werden.	ja	ja	ja	ja