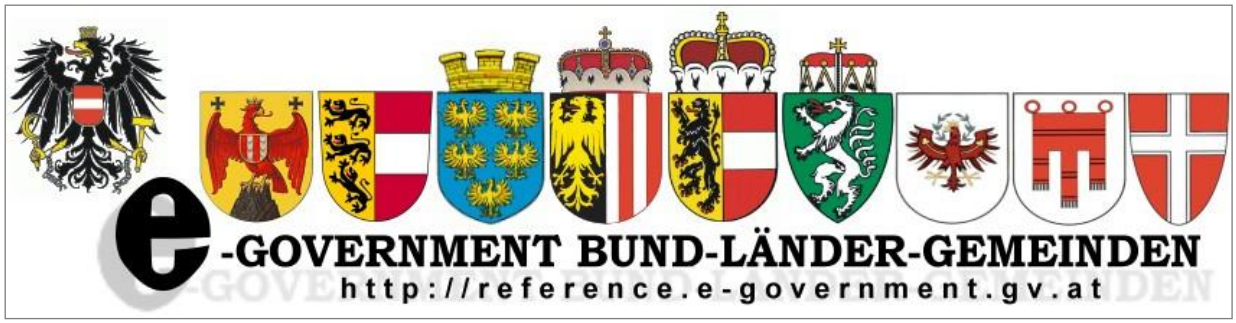

1

Portalverbund **Sicherheitsmaßnahmen** **(Algorithmen)**		**PVP-SMA** **1.4** **Ergebnis der Arbeitsgruppe**
Kurzbeschreibung	Dieses Dokument spezifiziert Sicherheitsmaßnahmen und Algorithmen für die Verwendung im Verwaltungsportalverbund oder kompatiblen Verbünden.	
Editor(en):	Peter Reif (Wien)	Projektteam / Arbeitsgruppe **AG Integration und Zugänge (AG-IZ)** AG-Leiter: Hannes Wittmann
Beiträge von:	Marco Ender (Wien), Sub-AG PVP / Sub-AG Policy	

2
3
4
5

Inhaltsverzeichnis

1 Gültigkeit des Dokuments

Dieses Dokument gilt ab dem Stichtag 10.6.2019, um eine Migration zu ermöglichen.

Danach sind verpflichtende Kriterien auf allen Anwendungsportalen einzuhalten (AWP darf nicht rot sein). Davon abweichende Einstellungen dürfen nach dem Stichtag ausnahmslos nur mehr auf zeitlich befristeten MigrationsAWP verwendet werden. Die Dauer des zeitlich befristeten Betriebs des MigrationsAWPs liegt dabei im Ermessen des AWP-Betreibers.

Für alle anderen Endpoints (STP, IDP und SP) ist im Rahmen der jährlichen Revision im Sinne der PVV eine entsprechende Selbstbewertung anhand dieses Dokuments sinngemäß durchzuführen.

2 Terminologie

Anforderungen in diesem Dokument werden mit in Großbuchstaben geschriebenen Schlüsselwörtern mit folgender Bedeutung definiert:

Kategorie	Schlüsselwörter	Schreibweise in [RFC2119]	Bedeutung
Verpflichtend	MUSS, DARF NICHT	MUST, MUST NOT	Unbedingt einzuhalten bzw. absolut verboten
Empfohlen	SOLL	SHOULD	Sicherheitstechnisch optimal

3 Farbschema zur Sicherheitsbewertung

Um PVP-Endpunkte - Anwendungsportale (AWP), Stammportale (STP) Serviceprovider (SP) und Identityprovider (IDP) – sicherheitstechnisch bewerten zu können, wird folgendes Farbschema definiert:

3.1 Rot: mindestens eine DARF NICHT Vorgabe ist verletzt

Der Endpunkt ist unsicher, weil praktikable Angriffe existieren oder es sich um ungenügend untersuchte Verfahren handelt. Eingehende Requests können auch mit sicherheitstechnisch unzulänglichen Parametern durchgeführt werden.

3.2 Gelb: mindestens eine eingeschränkt sichere Vorgabe wird unterstützt

Der Endpunkt ist eingeschränkt sicher und nicht rot eingestuft. Eingehende Requests können auch mit sicherheitstechnisch nicht optimalen Parametern durchgeführt werden. Eine Herabstufung der angeführten Algorithmen und Protokolle auf rot ist jederzeit möglich.

3.3 Grün: empfohlene Vorgaben werden unterstützt

Der Endpunkt ist sicher und wurde weder rot noch gelb eingestuft. Eingehende Requests können mit empfohlenen, sicherheitstechnisch optimalen Parametern durchgeführt werden.

3.4 Nicht klassifizierte Algorithmen und Protokolle

Der Einsatz von nicht klassifizierten Algorithmen und Protokollen ist außerhalb des Ampelsystems und wird von der AG-Policy im Anlassfall bewertet.

Stammportale (STP) und Identitätsprovider (IDP) können ebenfalls – z.B. für Revision – nach dem Farbschema beurteilt werden.

Die Einzelvorgaben sind sinngemäß mit den zugehörigen Farben markiert.

4 Algorithmen für XMLDsig/XMLEnc (SAML)

4.1 Vorgaben zu Algorithmen für XML-Signatur

Folgende Signatur- und Digest-Algorithmen für die Erstellung von XML-Signaturen nach [XMLSig] sind zu unterstützen. Andere Algorithmen DÜRFEN NICHT verwendet werden.

URI	Quelle	Bewertung
http://www.w3.org/2001/04/xmldsig-more#rsa-sha256	[RFC6931]	grün
http://www.w3.org/2001/04/xmldsig-more#rsa-sha512	[RFC6931]	grün
http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256	[RFC4051]	grün
http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha512	[RFC6931]	grün
http://www.w3.org/2001/04/xmlenc#sha256	[XMLEnc]	grün
http://www.w3.org/2001/04/xmlenc#sha512	[XMLEnc]	grün
http://www.w3.org/2001/04/xmlenc#ripemd160	[XMLENC]	grün

4.2 Vorgaben zu Algorithmen für XML-Encryption

Folgende Algorithmen für die Verschlüsselung von XML-Infosets nach [XMLEnc] sind zu unterstützen. Andere Algorithmen DÜRFEN NICHT verwendet werden.

URI	Quelle	Bewertung
http://www.w3.org/2001/04/xmlenc#aes128-cbc	[XMLEnc]	gelb*
http://www.w3.org/2001/04/xmlenc#aes256-cbc	[XMLEnc]	gelb*
http://www.w3.org/2009/xmlenc11#aes128-gcm	[XMLEnc11]	grün
http://www.w3.org/2009/xmlenc11#aes256-gcm	[XMLEnc11]	grün
http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p	[XMLEnc11]	grün
http://www.w3.org/2009/xmlenc11#ECDH-ES	[XMLEnc11]	grün

*) Diese Algorithmen werden als suboptimal bewertet, bessere Alternativen sind allerdings nicht allgemein verfügbar. Der jeweilige Portalbetreiber kann je nach der Struktur seiner Kommunikationspartner entscheiden, ob er diese als suboptimal eingestuften Algorithmen unterstützt. Die Verwendung ist aber in der Konfiguration nur so lange zu erlauben, wie es notwendig ist.

5 HTTP und HTTPS

Verbindungen von und zu PVP-Endpoints (STP, AWP, IDP und SP) DÜRFEN NICHT über unverschlüsseltes HTTP erfolgen. Ausnahmen sind ausreichen geschützte Verbindungen in internen Netzwerken und localhost-Verbindungen.

Bei Verwendung von HTTPS gelten die Vorgaben für TLS-Konfiguration.

6 Vorgaben für TLS-Konfiguration

6.1 Ziel

Ziel ist die sichere Kommunikation mit PVP-Endpunkten durch Anwendung der in diesem Dokument vorgegebenen TLS-Konfiguration.

6.2 Vorgaben

Die Spaltenüberschriften entsprechen der Beschreibung gemäß Kapitel 3.

	Rot	**Gelb**	**Grün**
Client- und Serverzertifikat	- RSA mit Schlüssellänge < 2048 Bit - Elliptische Kurven mit Schlüssellänge < 224 Bit		- RSA mit Schlüssellänge ≥ 2048 Bit - Elliptische Kurven mit Schlüssellänge ≥ 256 Bit
	MD5 Fingerprint	SHA-1 Fingerprint	SHA-256 oder SHA-512 Fingerprint
Protokoll	SSL 2.0 SSL 3.0 TLS 1.0 TLS 1.1		TLS 1.2 TLS 1.3
Schlüsselaustausch	Diffie-Hellman mit Schlüssellänge < 1024 Bit	Diffie-Hellman mit Schlüssellänge 1024 Bit ohne eigener Diffie-Hellman Gruppe	Diffie-Hellman mit Schlüssellänge ≥ 2048 Bit oder 1024 Bit mit eigener Diffie-Hellman Gruppe
	Elliptische Kurven mit Schlüssellänge < 224 Bit		Elliptische Kurven mit Schlüssellänge ≥ 256 Bit
	FORTEZZA KRB5 KRB5_EXPORT N/A NONE NULL PSK RSA_EXPORT RSA_EXPORT1024 SRP VKOGOSTR34.10-2001	DH ECDH RSA RSA_FIPS	DHE ECDHE

	VKOGOSTR34.10-94		
Authentifizierung	Anon DSS DSS_EXPORT KEA KRB5 KRB5_EXPORT N/A NONE NULL PSK RSA_EXPORT RSA_EXPORT 1024 RSA_FIPS VKO GOST R 34.10-2001 VKO GOST R 34.10-94	SHA	ECDSA RSA
Symmetrischer Cipher	Effektive Schlüssellänge < 128 Bit		Effektive Schlüssellänge ≥ 128 Bit
	3DES_EDE_CBC DES_192_EDE3_CBC DES_64_CBC DES_CBC DES_CBC_40 DES40_CBC FORTEZZA_CBC GOST28147 IDEA_128_CBC IDEA_CBC NONE NULL RC_CBC_40 RC2_128_CBC RC2_128_CBC_EXPORT40 RC2_CBC_128_CBC RC2_CBC_40 RC4 RC4_128 RC4_128_EXPORT40 RC4_40 RC4_56 RC4_64 SEED_CBC		AES_128_CBC AES_128_CCM AES_128_CCM_8 AES_128_GCM AES_256_CBC AES_256_CCM AES_256_CCM_8 AES_256_GCM ARIA_128_CBC ARIA_256_CBC CAMELLIA_128_CBC CAMELLIA_128_GCM CAMELLIA_256_CBC CAMELLIA_256_GCM ChaCha20_Poly1305
Hashalgorithmus	GOST28147 GOSTR3411 MD5 NONE NULL	SHA	SHA256 SHA384

6.3 Empfohlene Deploymentkonfiguration

Um die Interoperabilität auf grüner Ampelstufe gewährleisten zu können, wird neben den grünen Vorgaben in obiger Tabelle zu Zertifikaten, Schlüsselaustausch und Schlüssellängen konkret die Unterstützung folgender Cipher-Suites empfohlen:

IANA-Code	OpenSSL-String	IANA Description
0xC0,0x30	ECDHE-RSA-AES256-GCM-SHA384	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
0x00,0x9F	DHE-RSA-AES256-GCM-SHA384	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
0xC0,0x2C	ECDHE-ECDSA-AES256-GCM-SHA384	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
0xC0,0x2F	ECDHE-RSA-AES128-GCM-SHA256	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
0x00,0x9E	DHE-RSA-AES128-GCM-SHA256	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
0xC0,0x2B	ECDHE-ECDSA-AES128-GCM-SHA256	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
0xC0,0x28	ECDHE-RSA-AES256-SHA384	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
0x00,0x6B	DHE-RSA-AES256-SHA256	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
0xC0,0x24	ECDHE-ECDSA-AES256-SHA384	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
0xC0,0x27	ECDHE-RSA-AES128-SHA256	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
0x00,0x67	DHE-RSA-AES128-SHA256	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
0xC0,0x23	ECDHE-ECDSA-AES128-SHA256	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256

Der OpenSSL-Cipher-String:

```
ECDHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-SHA384:DHE-RSA-AES256-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256
```

Um die Interoperabilität mit Systemen zu ermöglichen, die keinen grünen Status erreichen, können zusätzlich folgende gelb bewerteten (sicherheitstechnisch nicht optimalen) Cipher-Suites eingesetzt werden:

IANA-Code	OpenSSL-String	IANA Description
0xC0,0x14	ECDHE-RSA-AES256-SHA	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
0x00,0x39	DHE-RSA-AES256-SHA	TLS_DHE_RSA_WITH_AES_256_CBC_SHA
0xC0,0x13	ECDHE-RSA-AES128-SHA	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
0x00,0x33	DHE-RSA-AES128-SHA	TLS_DHE_RSA_WITH_AES_128_CBC_SHA
0x00,0x35	AES256-SHA	TLS_RSA_WITH_AES_256_CBC_SHA
0x00,0x2F	AES128-SHA	TLS_RSA_WITH_AES_128_CBC_SHA

Der OpenSSL-Cipher-String (ohne den bereits oben eingebundenen grünen Ciphern):

```
ECDHE-RSA-AES256-SHA:DHE-RSA-AES256-SHA:ECDHE-RSA-AES128-SHA:DHE-RSA-AES128-SHA:AES256-SHA:AES128-SHA
```

6.4 Weiterführende Informationen und Quellen

https://www.onlinesicherheit.gv.at/nationale_sicherheitsinitiativen/weiterfuehrende_informationen/publikationen/144084.html
https://datatracker.ietf.org/doc/draft-ietf-uta-tls-bcp/
https://bettercrypto.org
http://demo.a-sit.at/wp-content/uploads/2014/11/Sicherheitsempfehlungen-TLS.pdf

7 Umsetzung auf Portalen

Folgende Möglichkeiten gibt es, Verbindungsanfragen von Clients die als gelb oder rot klassifiziert sind zu behandeln:

1. Verbindungen werden auf Protokollebene abgewiesen
2. Verbindungen werden angenommen und auf eine zentrale Fehlerseite weitergeleitet,

ein Zugriff auf die Anwendung ist nicht möglich

3. Verbindungen werden zur Anwendung durchgelassen, die Anwendung zeigt eine Information an.
4. Verbindungen werden zur Anwendung durchgelassen.

Für rote Verbindungen sind nur Möglichkeiten 1 und 2 zulässig. Die Varianten 2 und 3 haben den Vorteil, dass Benutzer gezielt mit Informationen versorgt werden können.

8 HTTP Methoden

Vorgaben für Methoden von HTTP Requests im Portalverbund, siehe [RFC2616].

8.1 Erlaubte Methoden

Requests mit folgenden HTTP-Methoden dürfen von Portalen im Portalverbund nicht prinzipiell geblockt werden:

GET, POST, PUT, DELETE, OPTIONS, HEAD

8.2 Verbotene Methoden

Requests mit folgenden HTTP-Methoden müssen von Portalen geblockt werden:

TRACK, TRACE

8.3 Weitere Methoden

Alle anderen Methoden sind im Anlassfall vom Anwendungsverantwortlichen mit den zugriffsberechtigten Stellen zu kommunizieren.

9 Referenzen

[RFC2119]	Key words for use in RFCs to Indicate Requirement Levels
[RFC2616]	Hypertext Transfer Protocol -- HTTP/1.1
[RFC6931]	Additional XML Security Uniform Resource Identifiers (URIs), April 2013
[XMLEnc]	XML Encryption Syntax and Processing, Dec. 2002
[XMLEnc11]	XML Encryption Syntax and Processing Version 1.1., April. 2013

10 Änderungshistorie

10.1 Version 1.3

Triple DES wird als unsicher eingestuft, die Ciphers 3DES_EDE_CBC und DES_192_EDE3_CBC wurden von gelb auf rot gesetzt, DES-CBC3-SHA wurde aus der gelben Deploymentkonfiguration entfernt.

10.2 Version 1.4

TLS 1.1 wird von gelb auf rot heruntergestuft. TLS 1.3 wird als neues Protokoll grün eingestuft.

Richtlinien über die Verwendung von HTTP Methoden.

Verwendung von HTTP.

Anwendung der Vorgaben auch auf STP, IDP und SP mit Umsetzungsvarianten.