7. November 2014 Studie · Web & Cloud · Digitale Identität · 12 Min. Lesezeit

HTTPS Analyse von GV.AT Domänen

Archiviert. Dieser Inhalt wird nicht mehr aktualisiert. Er bleibt zur Information verfügbar.

Quelle https://technology2.a-sit.at/veroeffentlichungen/https-analyse-von-gv-at-domaenen/

In diesem Projekt wurden die Eigenschaften von österreichischen **gv.at** Domänen analysiert. Der Fokus wurde dabei auf die Unterstützung von TLS (Anbieten der Dienste über HTTPS) gelegt. Im Rahmen dieses Projekts wurde das Rahmenwerk für die automatische Analyse geschaffen und die ersten Ergebnisse im Rahmen einer Kurzstudie präsentiert.

Im Folgenden wird eine kurze Zusammenfassung der wichtigsten Fakten gegeben (Beachten Sie, dass es sich um eine Analyse aus 2014 handelt. Die Verteilung hat sich seither sehr wahrscheinlich verändert):

- Es wurden 1285 Dienste analysiert, 763 davon unterstützten das HTTPS-Protokoll nicht.
- Bei den 522 Services, die HTTPS anbieten, ergibt sich folgendes Bild:
- Davon bieten 59 Services dediziert HTTPS an. Bei den anderen 463 Diensten handelt es sich um providerspezifsche Standardseiten oder Dienste die nicht für das Anbieten über HTTPS gedacht sind, aber ein Test-Zertifikat verwenden.
- Die Services wurden vor allem auf die verwendeten TLS-Ciphersuites analysiert, da diese maßgeblich die Sicherheit der aufgebauten TLS-Verbindungen beeinflussen:

Alle Details dazu finden Sie im Projektbericht.

Verwendung von SHA-1 in Zertifikaten

Mehrere Hersteller von Web-Browsern beabsichtigen, den weit verbreiteten Hash-Algorithmus durch neuere Alternativen abzulösen. Dazu wurden Richtlinien beschlossen, die ein schrittweises Auslaufen der Unterstützung von SHA-1 in Web-Browser vorsehen.

Die nachfolgende Tabelle illustriert die Unterstützung von SHA-1 in chronologischer Hinsicht und zeigt die Behandlung in den jeweiligen Web-Browsern an (Situation 2014). Die unterschiedliche Behandlung von SHA-1 wird in Etappen unterteilt und in der Grafik farblich kenntlich gemacht:

Hinweis (grün), Warnung (gelb) und Eskalation (rot).

Im Rahmen der HTTPS-Analyse wurde erhoben, welche Signaturalgorithmen die Webseiten öffentlicher Institutionen verwenden. Dabei wurden folgenden Kennzahlen festgestellt (zum Zeitpunkt der Analyse 2014):

- Bei 41 Servern ist das aktuell verwendete Zertifikat bereits vor 1.1.2016 nicht mehr gültig.
- 21 der 91 Zertifikate sind auch im Jahr 2016 noch gültig. Web-Browser werden betroffene Server als sicher, jedoch problembehaftet behandlen.
- 27 verbleibende Zertifikate sind auch nach 1.1.2017 noch gültig und werden ab dem Erscheinen von Google Chrome in Version 40 wie ungeschützte Verbindungen angezeigt.

Eine detaillierte Beschreibung der einzelnen Stufen und eine genaue Auflistung der untersuchten Zertifikate, sind im vollständigen Bericht einsehbar.

1. Einleitung

Der Algorithmus SHA-1 transformiert einen beliebigen Wert zu einer eindeutigen, irreversiblen Repräsentation (sog. „Hash value“). Die Hash-Funktion wurde 1995 von NIST im Standard FIPS PUB 180-1 standardisiert und findet seither weit verbreitet Anwendung. Insbesondere SSL- bzw. TLS-Zertifikate sind oftmals mit SHA-1 signiert, nachdem 2009 aufgezeigt wurde, dass MD5 hierfür keine ausreichende Sicherheit mehr bieten kann [1].

Im Jahr 2005 wurden die ersten erfolgreichen Angriffe auf SHA-1 präsentiert [2] [3]. Seither wurden stets effizientere Attacken erarbeitet, die jeweils Anlass dazu geben, alternative Verfahren in Betracht zu ziehen, die den aufgefundenen Problemen nicht ausgesetzt sind.

Um Auswirkungen eines künftig auch praktisch durchführbaren Angriffs bei SHA-1 frühzeitig entgegen zu wirken, beabsichtigten Browserhersteller eine schnelle Abkehr vom problembehafteten Algorithmus. Insbesondere angesichts der Tatsache, dass TLS-Zertifikate üblicherweise für einen Zeitraum von 1-3 Jahren ausgegeben werden, erscheint eine zeitnahe Reaktion sinnvoll.

2. Chronologie

Da erfolgreiche Angriffe auf SHA-1 weitreichende Folgen hätten, verfolgen mehrere Browser-Hersteller frühestens seit Ende 2013 jeweils autonome Richtlinien um Certificate Authorities (CA) und Kunden aktiv dazu zu animieren, auf Zertifikate mit SHA-2 umzusteigen.

Daraus abgeleitet können mehrere Etappen definiert werden, in denen die Verwendung von Zertifikaten mit SHA-1-Signatur unterschiedlich behandelt wird:

- Kein Vermerk: Die Verwendung von Zertifikaten mit SHA-1 wird nicht explizit gekennzeichnet.
- Hinweis: Der Browser weist darauf hin, dass SHA-1 verwendet wird. Die TLS-Verbindung wird jedoch als sicher erachtet.

- Warnung: Der Browser warnt davor, dass eine TLS-Verbindung zu einem Server hergestellt werden soll, der ein SHA-1-Zertifikat verwendet. Obwohl eine geschützte Verbindung aufgebaut werden kann, ist das erreichbare Sicherheitsniveau vergleichbar mit jenem von ungeschützten HTTP-Verbindungen.
- Eskalation: TLS-Verbindungen zu Server mit SHA-1-Zertifikat werden zurückgewiesen und behandelt wie nicht vertrauenswürdige Verbindungen. Durch eine entsprechende Meldung kennzeichnen Browser diese Verbindungen ausdrücklich als unsicher.

In der folgenden Tabelle werden diese Stufen in einer terminlichen und produktbezogenen Relation verwendet um die Unterstützung von SHA-1 zu kennzeichnen.

26.9.2014 [1] 7.11.2014 [2] Q1 2015 1.1.2016 1.1.2017

Microsoft Windows3		**Col3**	**Col4**	**Col5**	**x**
Mozilla Firefox4				Individuell	x
Google Chrome5			Individuell	Individuell	x

Tabelle 1. SHA-1 Unterstützung im zeitlichen Kontext. 1 Bzw. mit dem Erscheinen von Google Chrome 39. 2 Bzw. mit dem Erscheinen von Google Chrome 40. 3 http://blogs.technet.com/b/pki/archive/2013/11/12/sha1-deprecation-policy.aspx 4 https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/ 5 http://googleonlinesecurity.blogspot.de/2014/09/gradually-sunsetting-sha-1.html Die angeführte Tabelle berücksichtigt jene Browser-Hersteller, die eine Erklärung über ihren Umgang mit SHA-1 kundgetan haben. Obwohl die jeweiligen Richtlinien in ihren Ausführungen sehr unterschiedlich sind, liegt dennoch bei allen dreien der Konsens vor, dass ab 1.1.2017 Zertifikate mit SHA-1-Signatur nicht mehr akzeptiert werden.

Gemäß den Richtlinien von Microsoft dürfen nach 1.1.2016 keine SHA-1-Zertifikate mehr ausgestellt werden. Bis spätestens 1.1.2017 müssen bereits bestehende ausgetauscht werden. Der Konzern sieht außerdem vor, im Juli 2015 die Richtlinien den dann vorliegenden Umständen anzupassen.

In Versionen von Mozilla Firefox, die ab ersten Quartal 2015 erscheinen, soll in der Web-Konsole gewarnt werden wenn eine Webseite ein Zertifikat mit SHA-1 verwendet. Für gewöhnliche Anwender ist diese Konsole üblicherweise nicht ersichtlich. Ab 1.1.2016 werden neu ausgestellte Zertifikate, die SHA-1 verwenden, abgelehnt und einer unsicheren Verbindung gleichgestellt. Ab 1.1.2017 betrifft das auch bereits früher ausgestellte Zertifikate, die formal noch länger gültig sind.

Google Chrome plant ab Version 39 einen gut sichtbaren Hinweis in Form einer Triangel anzuzeigen sofern ein SHA-1-Zertifikat nach 1.1.2017 noch gültig ist. Ab Chrome 40 werden jene SHA-1-Zertifikate mit einer Triangel vermerkt, die zwischen 1.6.2016 und 31.12.2016 noch gültig sind. TLS-Verbindungen, deren SHA-1-Zertifikate auch 2017 noch gültig sind, werden dargestellt wie ungeschützte HTTP-Verbindungen. Ab der Freigabe von Chrome 41 im ersten Quartal 2015, werden auch SHA-1-Zertifikate mit einer Triangel gekennzeichnet, die zwischen 1.1.2016 und 31.12.2016 noch gültig sind. SHA-1-Zertifikate, die auch 2017 noch gültig sind, werden dann als ausdrücklich unsicher gekennzeichnet.

2.1. Unterstützung von SHA-256

Wenn SHA-1-Zertifikate gegen neuere ausgetauscht werden, sollte darauf geachtet werden, dass ein modernes Hashverfahren wie SHA-256 verwendet wird. Wie von einer bekannten Zertifizierungsstelle evaluiert wurde, sollten die gängigsten Betriebssysteme in den aktuellen Versionen mit SHA-256-Zertifikaten umgehen können [6] . Als untere Kompatibilitätsgrenze wurde angeführt, dass der Hashalgorithmus vor Microsoft Windows XP mit Service Pack 3 bzw. Apple OS X 10.5 nicht unterstützt wird.

3. Österreichische E-Government-Domains

In einer im September 2014 durchgeführten Untersuchung österreichischer .gv.at-Domains im Hinblick auf sicherheitskritische Aspekte, wurde auch erhoben, welche Signaturalgorithmen von den jeweiligen Webseiten verwendet werden. Angesichts der geplanten Abkehr von SHA-1-Zertifikaten sind auch mehrere Domains öffentlicher Einrichtungen betroffen.

Im Anhang A dieses Dokuments werden 91 untersuchte gv.at-Domains aufgelistet, die ein gültiges SHA-1-Zertifikat verwenden:

- Bei 41 davon ist das aktuell verwendete Zertifikat bereits vor 1.1.2016 nicht mehr gültig. Im Zuge einer Erneuerung sollte demnach darauf geachtet werden, dass fortan SHA-256 verwendet wird.
- 21 der 91 Zertifikate sind auch im Jahr 2016 noch gültig. Das bedeutet, dass mit der Freigabe von Google Chrome in Version 41 (Q1 2015) ein Hinweis angezeigt wird, der kenntlich macht, dass die Seiten sicher, aber problembehaftet sind.
- 27 verbleibende Zertifikate sind auch nach 1.1.2017 noch gültig und werden mit dem Erscheinen von Google Chrome in Version 40 (7.11.2014) gleich wie ungeschützte HTTP-Verbindungen angezeigt. Ab Version 41 werden TLS-Verbindungen zu den betroffenen Domains explizit als unsicher gekennzeichnet.

6 https://support.globalsign.com/customer/portal/articles/1499561-sha-256-compatibility Für Vergleichszwecke werden in Anhang B jene analysierten Domains angeführt, die ein gültiges SHA-256-Zertifikat verwenden. Technisch war eine TLS-Verbindung mit 472 Domains möglich; allerdings haben lediglich 95 Domains alle Anforderungen erfüllt um von gängigen Web-Browser nicht ohnehin als ungültig zurückgewiesen zu werden.

4. Fazit

Die schrittweise Einstellung der Akzeptanz von Zertifikaten mit SHA-1 soll dazu dienen, möglicherweise erfolgreichen Angriffen auf den Hashalgorithmus zuvor zu kommen. Da in aktuellen Betriebssystemen die Unterstützung von modernen Hashverfahren wie SHA-256 gegeben ist, sollten entsprechende Zertifikate anstandslos funktionieren.

Die Analyse von gv.at-Domains hat aufgezeigt, dass die Verwendung von SHA-1-Zertifikaten der momentan üblichen Praxis entspricht. Spätestens mit dem Erscheinen von Google Chrome 40 sind erste Implikationen bei 27 Domains öffentlicher Institutionen zu beobachten. Da sich alle Browser-Hersteller vorbehalten, im Falle erfolgreicher Angreife auf SHA-1 die Umstellungszeiträume vorzuziehen, kann ein zeitnaher Wechsel zu SHA-256-Zertifikaten als sehr empfehlenswert angesehen werden.

5. Literaturverzeichnis

[1] M. Stevens, A. Sotirov, J. Appelbaum, A. Lenstra, D. Molnar, D. A. Osvik und B. d. Weger, „Short Chosen-Prefix Collisions for MD5 and the Creation of a Rogue CA Certificate," *Cryptology ePrint Archive, Report 2009/111,* 2009.

[2] V. Rijmen und E. Oswald, „Update on SHA-1," *CT-RSA,* 2005.

[3] X. Wang, Y. Hongbo und Y. L. Yin, „Finding collisions in the full SHA-1," *CRYPTO,* 2005.

[4] E. Barker und A. Roginsky, „Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths," *NIST Special Publication 800-131A,* 2011.

[5] P. Teufl, A. Reiter, A. Marsalek und S. Kreuzhuber, „Kurzstudie HTTPS (SSL, TLS) Analyse österreichischer GV.AT Domänen," *A-SIT,* 2014.

Anhang A: gv.at Domains mit validen SHA-1-Zertifikaten Reihung nach Gültigkeitsdatum

Index	Hostname	Zertifizierungsstelle	Gültigkeitsdatum
1	www.staedtebund.gv.at	Thawte DV SSL CA, Thawte	14.12.2014 00:59:59
2	www.usp.gv.at	TERENA SSL CA, TERENA	04.01.2015 00:59:59
3	www.fundamt.gv.at	Go Daddy Secure Certification Authority, GoDaddy.com	15.01.2015 14:23:35
4	www.onlinesicherheit.gv.at	Thawte SSL CA, Thawte	19.02.2015 00:59:59
5	www.arbeitsinspektion.gv.at	a-sign-SSL-03, A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH	09.03.2015 13:43:56
6	www.neunkirchen.gv.at	EuropeanSSL Server CA, EUNETIC GmbH	07.04.2015 01:59:59
7	fma-va.brz.gv.at	Thawte SSL CA, Thawte	13.04.2015 01:59:59
8	e-begutachtung.brz.gv.at	Thawte SSL CA, Thawte	21.04.2015 01:59:59
9	english.bmf.gv.at	Thawte SSL CA, Thawte	25.04.2015 01:59:59
10	www.brz.gv.at	Thawte SSL CA, Thawte	25.04.2015 01:59:59
11	service.bmf.gv.at	Thawte SSL CA, Thawte	26.04.2015 01:59:59
12	appointment.bmeia.gv.at	VeriSign Class 3 Secure Server CA - G3, VeriSign	27.04.2015 01:59:59
13	www.verbrauchergesundheit.gv.at	Thawte SSL CA, Thawte	08.05.2015 01:59:59
14	www.strahlenregister.gv.at	Go Daddy Secure Certification Authority, GoDaddy.com	09.05.2015 16:28:07
15	hundestaffel.tbw.gv.at	RapidSSL CA, GeoTrust	13.05.2015 04:28:20
16	www.hundestaffel.tbw.gv.at	RapidSSL CA, GeoTrust	13.05.2015 04:28:20
17	www.tbw.gv.at	RapidSSL CA, GeoTrust	13.05.2015 04:28:20

Index	Hostname	Zertifizierungsstelle	Gültigkeitsdatum
18	egov.graz.gv.at	VeriSign Class 3 Secure Server CA - G3, VeriSign	01.06.2015 01:59:59
19	katplan.bgld.gv.at	DigiCert High Assurance CA-3, DigiCert Inc	01.06.2015 14:00:00
20	wahl.bgld.gv.at	DigiCert High Assurance CA-3, DigiCert Inc	01.06.2015 14:00:00
21	geodaten.bgld.gv.at	DigiCert High Assurance CA-3, DigiCert Inc	01.06.2015 14:00:00
22	portal.bgld.gv.at	DigiCert High Assurance CA-3, DigiCert Inc	01.06.2015 14:00:00
23	apps.bgld.gv.at	DigiCert High Assurance CA-3, DigiCert Inc	01.06.2015 14:00:00
24	www.noe.gv.at	a-sign-SSL-03, A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH	18.06.2015 13:45:47

25	**sterztest.stmk.gv.at**	**Thawte SSL CA, Thawte**	**04.08.2015 01:59:59**
26	projekt.ssr-wien.gv.at	Go Daddy Secure Certification Authority, GoDaddy.com	16.08.2015 12:42:39
27	bewerbung.ssr-wien.gv.at	Go Daddy Secure Certification Authority, GoDaddy.com	16.08.2015 12:42:39
28	smonline.ssr-wien.gv.at	Go Daddy Secure Certification Authority, GoDaddy.com	16.08.2015 12:42:39
29	erlaesse.ssr-wien.gv.at	Go Daddy Secure Certification Authority, GoDaddy.com	16.08.2015 12:42:39
30	service.ssr-wien.gv.at	Go Daddy Secure Certification Authority, GoDaddy.com	16.08.2015 12:42:39
31	webservice.ssr-wien.gv.at	Go Daddy Secure Certification Authority, GoDaddy.com	16.08.2015 12:42:39
32	pallast.stmk.gv.at	a-sign-SSL-03, A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH	14.09.2015 17:19:56
33	www.bregenz.gv.at	Thawte SSL CA, Thawte	19.10.2015 01:59:59
34	www.elga-online.gv.at	VeriSign Class 3 Extended Validation SSL SGC CA, VeriSign	24.10.2015 01:59:59
35	www.gesundheit.gv.at	TERENA SSL CA, TERENA	27.10.2015 00:59:59
36	en.brz.gv.at	Thawte SSL CA, Thawte	29.10.2015 00:59:59
37	www.bmf.gv.at	Thawte SSL CA, Thawte	29.10.2015 00:59:59
38	www.klimafonds.gv.at	COMODO High-Assurance Secure Server CA, COMODO CA Limited	20.11.2015 00:59:59
39	klimafonds.gv.at	COMODO High-Assurance Secure Server CA, COMODO CA Limited	20.11.2015 00:59:59
40	www.land-oberoesterreich.gv.at	TERENA SSL CA, TERENA	17.12.2015 00:59:59
41	www.bfg.gv.at	Thawte SSL CA, Thawte	23.12.2015 00:59:59
42	www.bvwg.gv.at	Thawte SSL CA, Thawte	08.01.2016 00:59:59

25	**sterztest.stmk.gv.at**	**Thawte SSL CA, Thawte**	**04.08.2015 01:59:59**
43	apps.egiz.gv.at	a-sign-SSL-03, A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH	27.01.2016 11:42:21
44	www.egiz.gv.at	a-sign-SSL-03, A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH	27.01.2016 12:14:08
45	demo.egiz.gv.at	a-sign-SSL-03, A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH	27.01.2016 12:19:32
46	www.vwgh.gv.at	Thawte SSL CA, Thawte	06.02.2016 00:59:59
47	webmail.bmeia.gv.at	VeriSign Class 3 Secure Server CA - G3, VeriSign	27.02.2016 00:59:59
48	www.oeffentlicherdienst.gv.at	TERENA SSL CA, TERENA	21.03.2016 00:59:59
49	www.jobboerse.gv.at	TERENA SSL CA, TERENA	21.03.2016 00:59:59
50	www.ersb.gv.at	TERENA SSL CA, TERENA	11.04.2016 01:59:59
51	amtssignatur.brz.gv.at	Thawte SSL CA, Thawte	21.04.2016 01:59:59
52	www.formularservice.gv.at	Thawte SSL CA, Thawte	05.05.2016 01:59:59
53	portal04.bmf.gv.at	Thawte SSL CA, Thawte	18.06.2016 01:59:59
54	www.e-shop.gv.at	Thawte SSL CA, Thawte	13.07.2016 01:59:59
55	www.sicherheitshandbuch.gv.at	a-sign-SSL-EV-03, A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH	15.07.2016 11:33:58

56	**www.data.gv.at**	**Thawte SSL CA, Thawte**	**07.08.2016 01:59:59**
57	www.stammzahlenregister.gv.at	TERENA SSL CA, TERENA	22.08.2016 01:59:59
58	www01.noel.gv.at	a-sign-SSL-03, A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH	17.10.2016 13:57:51
59	portal.linz.gv.at	Thawte SSL CA, Thawte	18.10.2016 01:59:59
60	geoshop.noel.gv.at	a-sign-SSL-03, A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH	19.10.2016 10:16:36
61	www.help.gv.at	a-sign-SSL-EV-03, A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH	22.10.2016 08:43:41
62	www.erb.gv.at	Thawte SSL CA, Thawte	23.11.2016 00:59:59
63	ams.brz.gv.at	Thawte SSL CA, Thawte	12.12.2016 00:59:59
64	www.bmbf.gv.at	TERENA SSL CA, TERENA	29.01.2017 00:59:59
65	www.lvwg-ooe.gv.at	TERENA SSL CA, TERENA	30.01.2017 00:59:59
66	www.bmlv.gv.at	TERENA SSL CA, TERENA	05.02.2017 00:59:59
67	teacher.lsr-t.gv.at	RapidSSL CA, GeoTrust	16.02.2017 05:00:25
68	nts.doris.bmvit.gv.at	TERENA SSL CA, TERENA	06.03.2017 00:59:59
69	www.ref.gv.at	a-sign-SSL-03, A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH	13.03.2017 07:42:35
70	bund.jobboerse.gv.at	TERENA SSL CA, TERENA	07.04.2017 01:59:59
71	www.bka.gv.at	TERENA SSL CA, TERENA	11.04.2017 01:59:59
72	heimtierdatenbank.ehealth.gv.at	TERENA SSL CA, TERENA	14.04.2017 01:59:59
73	www.bmvit.gv.at	TERENA SSL CA, TERENA	15.04.2017 01:59:59

56	**www.data.gv.at**	**Thawte SSL CA, Thawte**	**07.08.2016 01:59:59**
74	www.lvwg-tirol.gv.at	TERENA SSL CA, TERENA	16.04.2017 01:59:59
75	lawine.tirol.gv.at	TERENA SSL CA, TERENA	16.04.2017 01:59:59
76	www.tirol.gv.at	TERENA SSL CA, TERENA	19.04.2017 01:59:59
77	www.innsbruck.gv.at	TERENA SSL CA, TERENA	08.05.2017 01:59:59
78	www.edusig.gv.at	a-sign-SSL-03, A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH	08.03.2018 13:26:39
79	info.lsr-ktn.gv.at	Go Daddy Secure Certification Authority, GoDaddy.com	21.03.2018 13:12:41
80	www.vfgh.gv.at	Thawte SSL CA, Thawte	02.09.2018 01:59:59
81	www.sozialinfo.noe.gv.at	a-sign-SSL-03, A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH	03.09.2018 12:28:17
82	portal.noe.gv.at	a-sign-SSL-03, A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH	28.11.2018 06:12:30
83	www.kalendarium.gv.at	a-sign-SSL-03, A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH	18.12.2018 08:19:23
84	www.dsb.gv.at	a-sign-SSL-03, A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH	30.12.2018 14:14:40
85	vollmachten.egiz.gv.at	a-sign-SSL-03, A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH	10.01.2019 11:02:37
86	www.bmwfw.gv.at	a-sign-SSL-03, A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH	20.02.2019 09:11:51

87	**www.hpa.gv.at**	**a-sign-SSL-03, A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH**	**14.04.2019 11:17:21**
88	www.bbg.gv.at	Bundesrechenzentrum CA, Bundesrechenzentrum GmbH	07.05.2019 15:05:20
89	stratfuelg.gv.at	EuropeanSSL Server CA, EUNETIC GmbH	17.06.2019 01:59:59
90	www.fma.gv.at	a-sign-SSL-03, A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH	02.07.2019 13:07:54
91	formulare.zmr.register.gv.at	a-sign-SSL-03, A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH	09.10.2019 09:32:31

Anhang B: gv.at Domains mit validen SHA-256-Zertifikaten Reihung nach Gültigkeitsdatum

Index	Hostname	Zertifizierungsstelle	Gültigkeitsdatum
1	fsw.amtsweg.gv.at	Go Daddy Secure Certificate Authority - G2, GoDaddy.com	22.02.2016 09:15:26
2	www.amtsweg.gv.at	Go Daddy Secure Certificate Authority - G2, GoDaddy.com	28.07.2016 15:50:31
3	www.parlament.gv.at	GlobalSign Extended Validation CA - SHA256 - G2, GlobalSign nv-sa	25.10.2016 10:50:05
4	www.vorarlberg.gv.at	thawte SSL CA - G2, thawte	28.04.2018 01:59:59