HADMÉRNÖK

XII. Évfolyam 2. szám – 2017. június

E-KORMÁNYZATI SZOLGÁLTATÁSOK KOMMUNIKÁCIÓBIZTONSÁGA

COMMUNICATION SECURITY OF E-GOVERNMENT SERVICES

SZÁDECZKY Tamás

(ORCID: 0000-0001-7191-4924)

szadeczky.tamas@uni-nke.hu

Absztrakt

A kormányzat az ország legnagyobb adatkezelője. Adatkezelési- és feldolgozási tevékenységüket törvényi felhatalmazás alapján, az adatvédelmi jogszabályoknak megfelelően végzik. A helyi adatvédelmi hatóság felelős a tevékenység felügyeletéért, de ennek keretében ritkán foglalkoznak az információbiztonsági jó gyakorlat által elvártakkal.

A tanulmány összehasonlító elemzés végez a német és a magyar e-kormányzati ügyfélszolgáltatások tekintetében. A kutatás központjában az állampolgár és a közigazgatási szerv közötti kommunikáció kriptográfiai algoritmusainak és protokolljainak analízise áll. Ez magában foglalja az általános közigazgatási portálok, valamint specifikus szolgáltatások, mint az adóügyi nyilvántartások rendszerét.

A téma aktualitását

A kutatás célja a nemzetközi jó gyakorlat meghatározása és így a jogalkalmazó felé az alkalmazandó technikai beállításokra vonatkozó javaslat bemutatása.

Kulcsszavak: *Elektronikus közszolgáltatások, Kommunikációs protokollok, Weblapok biztonsága*

Abstract

The government is the largest data controller of a country. Their data controlling- and processing activities are authorized by the law and done according the data protection regulation. The local data protection authority is typically in charge to overview this process. As they are in charge of the legal issues, but hardly ever deal with the information security best practices.

The paper is about a comparative research of the communication security of e-Government services in Germany and Hungary. The focus point of the research is to analyze the cryptographic security algorithms and protocols which encrypt the communication in the relations of the citizen and a governmental body. This includes the general e-Government portals, central authorities and specialized services, like income tax reporting solutions.

The goal of the research is to provide a best practice usable for governmental communication based on international standards and current practices.

Keywords: *Electronic public services, Communication protocols, Webpage security*

A kézirat benyújtásának dátuma (Date of the submission): 2017.04.22.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.05.24.

BEVEZETÉS

Ahogy azt a szerző korábbi tanulmányában [1] kifejtette, a kriptográfiai algoritmusok és protokollok sérüléseiből, illetve elavulásából adódó átállási feladatokat – amelyek egyébként minden informatikai üzemeltetőre és alkalmazóra feladatot rónak – a szabványalkotók és hatóságok mindössze kis hányada kezeli. Ennek oka egyrészről a szabályozásban általában elvárt technológiai függetlenség, másrészről a technikai változások üzleti szempontból történő lekövetésének gyakorlati nehézségei, ahogy azt a PCI DSS SSL és korai TLS verzióváltással kapcsolatos felhasználói ellenállása és az átállási idő módosítása is mutatja.

A jelen kutatás[1] keretében az elektronikus kormányzati szolgáltatások ügyfélportál-állampolgár viszonylatú kommunikációja során alkalmazott algoritmusok és protokollok megfelelősége kerül vizsgálatra. További fontos kutatási irány lehet még az e-kormányzati szolgáltatások egymás közötti adatcseréje, illetve az együttműködési képesség érettségének értékelése. [2]

A VIZSGÁLT RENDSZEREK

A kutatás során a Német Szövetségi Köztársaság és Magyarország egyes kiválasztott, azonos e-közigazgatási funkciót betöltő általános- illetve szakigazgatási rendszerei kerültek összehasonlításra. Minden esetben a közvetlen ügyfélkapcsolatot lehetővé tévő, legalább az egyik országban személyes adat kezelését, továbbítását végző rendszerek kerültek vizsgálat alá. A vizsgálat során az adott rendszereknek a kommunikációs protokoll-megfelelőségi értékelése került elvégzésre. A munka során az 1. táblázat szerinti rendszerek képezték a vizsgálat tárgyát.

Funkció	**Magyar rendszer**	**Német rendszer**
Általános e-közigazgatás	Ügyfélkapu	Bürgerserviceportal
Adóügyi igazgatás	Ügyfélkapu	ELSTER Online
Erkölcsi bizonyítvány	Webes ügysegéd, KAÜ	Bundesamt für Justiz – Führungszeugnis

1. táblázat: vizsgált rendszerek (saját szerkesztés)

A VIZSGÁLT PARAMÉTEREK

A HTTPS kommunikáció a weblapok megtekintésének biztonságos módja, amely titkosított kapcsolatot hoz létre a webszerver és a kliensoldali böngésző között. Viszont a kiválasztható protokollok, algoritmusok és paraméterek olyan sokrétűek, hogy hibás- vagy kevéssé biztonságos beállítás valószínűsége igen nagy.

A HTTPS biztonságának első lépése a szerver nyilvános kulcsú infrastruktúra (Public Key Infrastructure, PKI) magánkulcsának a védelme, ugyanis ez azonosítja magát a szervert. Itt elvárható a legalább 2048 bites modulus-méretű RSA kulcsok, és legalább az SHA-256 hash

[1] A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés” elnevezésű kiemelt projekt keretében működtetett Zrínyi Miklós Habilitációs Program keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült.

algoritmus használata. Ez mindenhol teljesült. A tanúsítvány kiadója megbízható kell legyen, tehát egy elismert hitelesítés-szolgáltató kell, hogy kiadja azt, bár a kérdés ennél komplexebb és formális vizsgálata nehézségekbe ütközik. [3] Előnyös lenne, ha a hagyományos helyett Extended Validation (EV) tanúsítványt alkalmaznának, ahol megtörténik a kérelmező jogi személy identitásának az ellenőrzése is, nem csak azt vizsgálják, hogy az igénylőnek a befolyása alatt áll az adott szerver. Az EV tanúsítványt a böngésző zöld címsora vagy más zöld mező jelzi. A kulcs és a tanúsítvány minden vizsgált rendszer esetén megfelelő volt. Egy esetben EV tanúsítványt használtak, ami előnyös, de pont ugyanebben az esetben merül fel a tanúsítvány kibocsátójával szembeni csökkent bizalom is.

A következő lépés a kommunikáció titkosítását végző protokoll verziója, amely lehet SSL 2.0, 3.0, TLS 1.0, 1.1 és 1.2. Az első két protokoll sérülékeny, azokat nem szabad használni. A TLS 1.0 használata már kerülendő, de sajnos sok esetben kompatibilitási okok miatt azt használni kell. A TLS 1.1 esetén a rossz konfigurációkat kerülni kell, a TLS 1.2 viszont minden esetben megfelelő. Alapvető problémaként említhetjük meg, hogy csak a már elavult TLS 1.0 protokollt alkalmazzák a magyar rendszerek közül kettőnél, illetve a TLS 1.0 még elérhető az újabb protokollok mellett 1-1 esetben.

A kulccscsere eljárások közül célszerű kizárólag az ECDHE (Elliptic Curve Diffie-Hellman Exchange, elliptikus görbéken alapuló Diffie-Hellman kucscsere) támogatása, ugyanis ez a modern eljárás teszi csak lehetővé a Forward Secrecy támogatását. [4] A Forward Secrecy azt biztosítja, hogy az esetlegesen feltört titkosítási kulccsal ne lehessen minden korábbi kommunikációt is megfejteni. Csak ECDHE vagy DHE kulcscsere esetén lehet beállítani.

A szimmetrikus kulcs mérete bitben 128 bit legyen AES algoritmus esetén, az ennél gyengébb 56, 112 bites rejtjelzések már nem tekinthetők biztonságosnak. Az RC4 algoritmus sérülékeny, az tilos használni, a 3DES algoritmus pedig elavult és lassú, ezért kerülendő.

A blokkrejtjelzési üzemmódok (block cipher mode of operation) közül a GCM (Galois Counter Mode) használata előnyös, javasolható. [5]

A HTTP Strict Transport Security (HTTP szigorú átviteli biztonság) beállítása esetén nem engedélyezett a nem titkosított kommunikáció a szerverrel, tehát nem lehetséges a korábban titkosítást megkövetelő honlaphoz titkosítás nélkül kapcsolódni. Ez a legfontosabb beállítandó paraméter. [6]

A VIZSGÁLATI ELJÁRÁS

A tesztek során kettő kísérlet került végrehajtásra. Egyrészről ugyanazon a napon (2017. február 25.) mind a hat rendszer HTTPS kommunikációjának részletes jellemzői és paraméterei kerültek elemzésre a Qualys SSL Labs rendszerében.[2] A Qualys a világ egyik piacvezető sérülékenység-elemző rendszerének gyártója. A Qualys SSL Labs szolgáltatás részletes technikai elemezést végez a titkosított kapcsolatot biztosító weblap HTTPS protokollja, algoritmusai és paraméterei tekintetében. A többoldalas részletes elemzés mellett, amelynek a legfontosabb eredményei a 2. táblázatban kerülnek összefoglalásra, az SSL Labs az összesített eredményt is megmutatja, amely minden ismertetett honlap estében egy-egy ábrán feltüntetésre került (ld. 1-6. ábrák). Az összesített eredmény a legfontosabb biztonsági jellemzők alapján ad egy besorolást, amely F-től (legrosszabb) A+-ig (legjobb) terjed. Itt cél a minél jobb eredmény elérése, bár önmagában a jó eredmény még nem jelent biztosítékot valamely követelmény-megfelelésre. Például a PCI DSS tiltja a TLS 1.0 használatát, de az

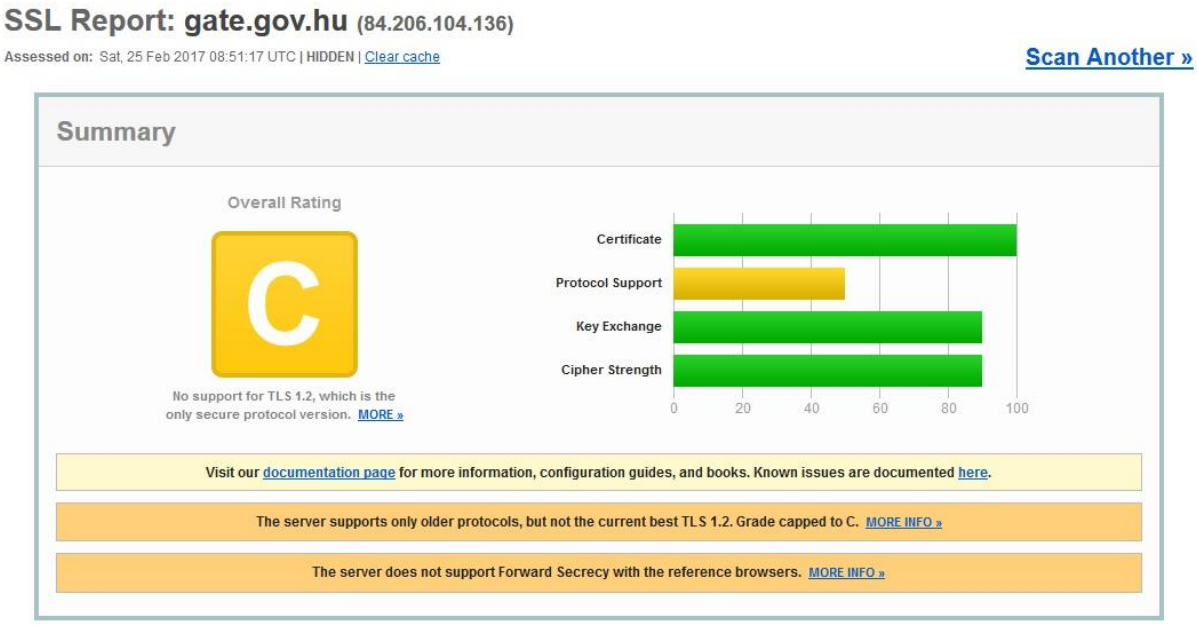
[2] Elérhető: https://www.ssllabs.com/ssltest/index.html [2017.03.19.]

SSL Labs nem rontja a honlap értékelését, ha a TLS 1.0 mellett a TLS 1.2 is elérhető a szerveren. A tesztek során kontrollvizsgálatként a Qualys SSL Labs legfőbb eredményei egy Windows 7 SP 1 (Build 7601) alatt futó Firefox 51.0.3 böngészővel is ellenőrzésre kerültek. Itt a kommunikáció során alkalmazott titkosítási csomagnak meg kellett egyeznie a SSL Labs által felismert, a szerveroldalon elsődlegesen preferált, legjobb biztonsági jellemzőjű HTTPS kommunikációs beállítással. Kontroll-ellenőrzésre került emellett a tanúsítvány kibocsátója, a magánkulcs modulusmérete és a tanúsítvány egyéb jellemzői (kibocsátó megbízhatósága, hash-algoritmus, validáció típusa).

ÖSSZEHASONLÍTÓ ELEMZÉS

Ügyfélkapu (magyarorszag.hu, gate.gov.hu)

A honlap az e-közigazgatás centralizált azonosító rendszere. A Magyarországon elérhető e-kormányzati szolgáltatások túlnyomó része ezen keresztül végzi az azonosítást. Kizárólag egyfaktoros tudás-alapú azonosítást használ. A jelszó maximális érvényessége 2 év. A szerver SLL tanúsítványát a Microsec e-Szigno SSL CA 2014 bocsátotta ki, ami egy Magyarországon működő hitelesítés-szolgáltató kibocsátója. A kontrollvizsgálat során alkalmazott titkosítási csomag: TLS_RSA_WITH_AES_128_CBC_SHA, 128 bites kulcs, TLS 1.0. A tesztek részletes eredményei a 2. táblázatban, összesített eredménye az 1. ábrán látható.



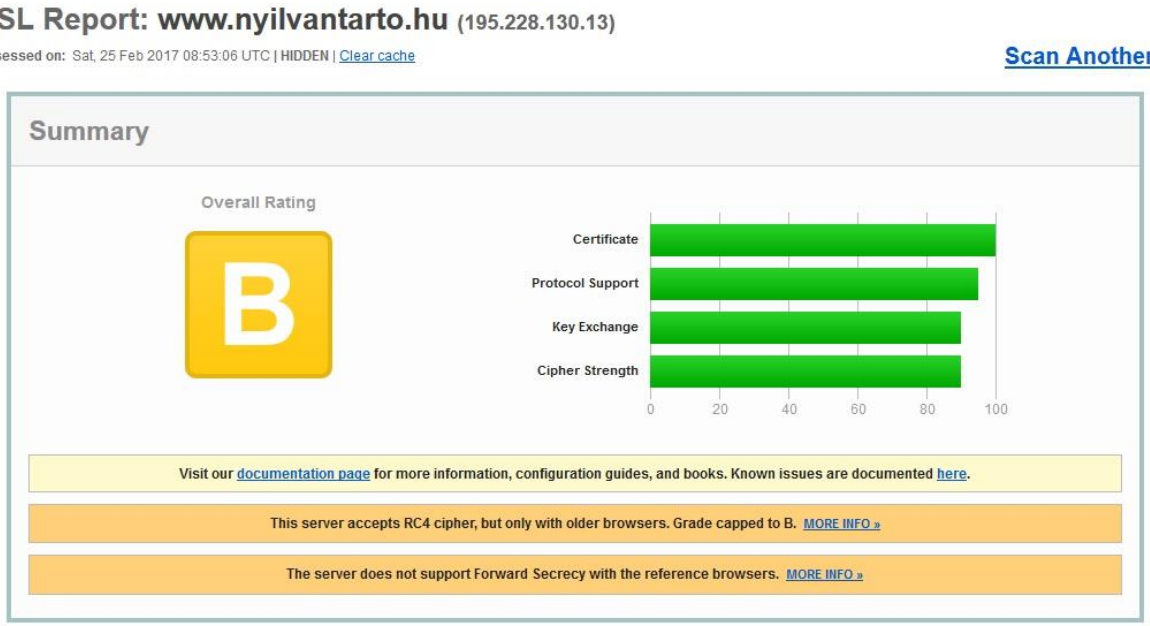
1. ábra: Ügyfélkapu SSL riportja[3]

Webes ügysegéd (www.nyilvantarto.hu/ugyseged/)

A webes ügysegéd az erkölcsi bizonyítvány, a járműigazgatás és a rendelkezési nyilvántartás ügyintézésére alkalmas. Azonosítása különbözik az ügyfélkapu azonosítási rendszerétől. Alapvetően a legjobb, TLS 1.2 protokollt alkalmazza a kommunikációhoz, de a korábbi verziók is elérhetőek. Az azonosítás az ügyfélkapuban használt felhasználónév jelszó párossal történik. Az alkalmazott tanúsítvány a biztonsági követelményeknek megfelelő, kibocsátója a

[3] Ábra forrása: Qualys SSL Labs https://www.ssllabs.com/ssltest/analyze.html?d=gate.gov.hu&hideResults=on [2017. 02. 25.]

Microsec e-Szigno SSL CA 2014, ami egy Magyarországon működő hitelesítés-szolgáltató. A kontrollvizsgálat során alkalmazott titkosítási csomag: TLS_RSA_WITH_AES_256_CBC_SHA, 256 bites kulcs, TLS 1.2. A tesztek részletes eredményei a 2. táblázatban, összesített eredménye az 2. ábrán látható.

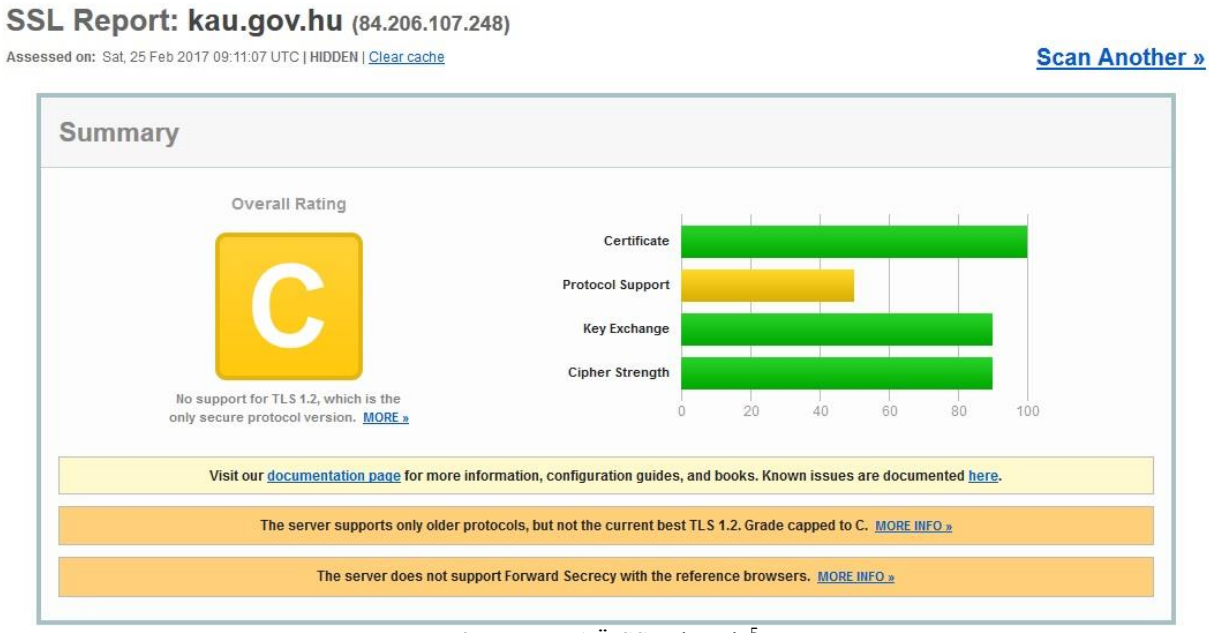


2. ábra: Nyilvántartó SSL riportja[4]

Központi Azonosítási Ügynök (KAÜ, kau.gov.hu)

A központi azonosítási ügynök a szabályozott elektronikus ügyintézési szolgáltatások (SZEÜSZ) egységes azonosító felülete. Az azonosítás történhet az ügyfélkapu felhasználónév-jelszó párossal, valamint az új típusú személyi igazolványban tárolt azonosító tanúsítvánnyal is. Sajnos ez utóbbi funkció egyelőre még nem működik. Annak ellenére, hogy ez a jövőbeli egységes azonosítási platform, sajnos pont ugyanazt az elavult protokollt és beállításokat használja az adatforgalom védelmére, mint az Ügyfélkapu. Az alkalmazott tanúsítvány a biztonsági követelményeknek megfelelő, kibocsátója a NetLock Expressz (Class C) Tanúsítványkiadó, ami egy Magyarországon működő hitelesítés-szolgáltató kibocsátója. A kontrollvizsgálat során alkalmazott titkosítási csomag: TLS_RSA_WITH_AES_128_CBC_SHA, 128 bites kulcs, TLS 1.0. A tesztek részletes eredményei a 2. táblázatban, összesített eredménye a 3. ábrán látható.

[4] Ábra forrása: Qualys SSL Labs https://www.ssllabs.com/ssltest/analyze.html?d=gate.gov.hu&hideResults=on [2017. 02. 25.]



3. ábra: KAÜ SSL riportja[5]

Bürgerserviceportal (www.buergerserviceportal.de)

Németországban nincsen olyan egységes általános e-közigazgatási portál, ami az ügyfélkapunak teljes mértékben megfeleltethető lenne. Amit itt vizsgálunk, az az egyes tartományi közigazgatási funkcióhoz való hozzáférést biztosító honlap. Ezen a portálon keresztül férhető hozzá a szövetségi államok ilyen típusú szolgáltatása, de a rendszer elkülöníti ezeket egymástól. A kommunikáció TLS 1.2 protokollal és megfelelően modern titkosítási algoritmussal működik. Az alkalmazott tanúsítvány az elérhető legnagyobb biztonságot nyújtja. Az azonosítás egyetlen lehetséges módja az új típusú személyi igazolványban (der neue Personalausweis, nPA) illetve az elektronikus tartózkodási engedélyben (elektronisches Aufenthaltstitel, eAT) megtalálható azonosítási tanúsítvánnyal lehetséges. Ezzel tehát mindenképpen kétfaktoros azonosítás valósul meg, ugyanis az okmányon lévő chipben tárolt tanúsítványhoz csak a PIN kód ismeretében lehet hozzáférni. Problémát jelent, hogy a szolgáltatások így nem olyan széles körben hozzáférhetőek, mint az ügyfélkapu esetében, hiszen az állampolgárnak rendelkeznie kell új típusú személyi igazolvánnyal, amelyen az elektronikus funkciókat aktiválnia kellett, valamint meghatározott típusú kártyaolvasóval is. Ez az azonosítási mód gyakorlatilag kizárja a Németországban élő külföldiek túlnyomó részét a szolgáltatásból. Az alkalmazott tanúsítvány kibocsátója a T-Systems International GmbH. A tesztek összesített eredménye a 4. ábrán látható.

Az alkalmazott tanúsítvány a biztonsági követelményeknek megfelelő, kibocsátója a T-Systems International GmbH, ami egy Németországban működő hitelesítés-szolgáltató. A kontrollvizsgálat során alkalmazott titkosítási csomag: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, 128 bites kulcs, TLS 1.2. A tesztek részletes eredményei a 2. táblázatban, összesített eredménye a 4. ábrán látható.

[5] Ábra forrása: Qualys SSL Labs https://www.ssllabs.com/ssltest/analyze.html?d=kau.gov.hu&hideResults=on [2017. 02. 25.]

4. ábra: Bürgerserviceportal SSL riportja[6]

ELSTER Online (www.elsteronline.de/eportal/)

Az adóigazgatási eljárásokban szövetségi szinten egységes rendszert használnak. Ezen a portálon keresztül lehet benyújtani a személyi jövedelemadó-bevallásokat, illetve egyéb adóügyi kérelmeket. A titkosítás még magasabb szintű, mint az előző szolgáltatásnál, ugyanis itt 256 bites AES kulcsot használnak. Ahogyan a teszteken is látható, jelentősebb konfigurációs problémáktól mentes a honlap beállítása. Az azonosítás az előzőekben leírt módon történik. A tanúsítvány kibocsátója a Symantec Class 3 EV SSL CA - G3. A tesztek összesített eredménye az 5. ábrán látható.

Az alkalmazott tanúsítvány a biztonsági követelményeknek megfelelő, kibocsátója a Symantec Class 3 EV SSL CA - G3, ami egy Egyesült Államokban működő hitelesítés-szolgáltató kibocsátója. Megbízhatóságát illetően a Google-nek erős kétségei vannak és várhatóan nem megbízhatónak fogja minősíteni a tanúsítványait. [7] A tanúsítvány kiadásakor ez a probléma még nem volt ismert. A kontrollvizsgálat során alkalmazott titkosítási csomag: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, 256 bites kulcs, TLS 1.2. A tesztek részletes eredményei a 2. táblázatban, összesített eredménye az 5. ábrán látható.

[6] Ábra forrása: Qualys SSL Labs
https://www.ssllabs.com/ssltest/analyze.html?d=www.buergerserviceportal.de&hideResults=on
[2017. 02. 25.]

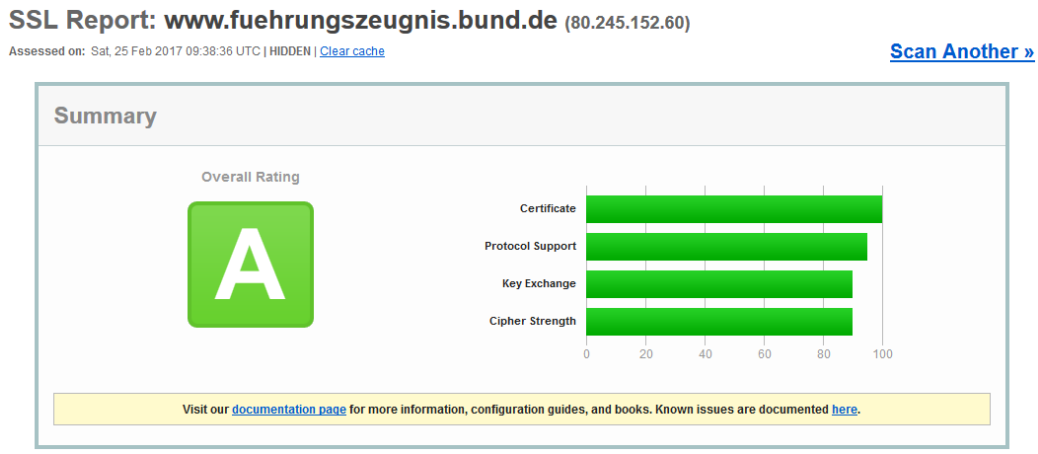
5. ábra: Elster Online SSL riportja[7]

Führungszeugnis (www.fuehrungszeugnis.bund.de/)

Az erkölcsi bizonyítványok kiadása iránti kérelem szövetségi szinten egységes rendszerben, a szövetségi igazságügyi hivatal weblapján történik, elektronikusan. Ez a honlap az adóügyi honlapnál már bemutatott protokollt és algoritmusokat használja, a honlap biztonsági beállításai itt is megfelelőek. Az azonosítás itt is az új típusú személyi igazolvánnyal történik.

Az alkalmazott tanúsítvány a biztonsági követelményeknek megfelelő, kibocsátója a Zentrum fuer Informationsverarbeitung und Informationstechnik ZIVIT CA - G01, ami egy Németországban működő állami hitelesítés-szolgáltató. A kontrollvizsgálat során alkalmazott titkosítási csomag: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, 256 bites kulcs, TLS 1.2. A tesztek részletes eredményei a 2. táblázatban, összesített eredménye a 6. ábrán látható.

[7] Ábra forrása: Qualys SSL Labs
https://www.ssllabs.com/ssltest/analyze.html?d=www.elsteronline.de&hideResults=on
[2017. 02. 25.]



6. ábra: Führungzeugnis.bund.de SSL riportja[8]

ÉRTÉKELÉS, KÖVETKEZTETÉSEK

A tesztek eredményeinek összehasonlítása a 2. táblázatban látható, míg a különböző paraméterek leírása

Az összesített eredmény a legfontosabb biztonsági jellemzők alapján ad egy besorolást, amely F-től (legrosszabb) A+-ig (legjobb) terjed.

Jellemző	ÜK	ÜS	KAÜ	BSP	EO	FZ
Tanúsítvány RSA modulusméret [bit]	2048	2048	2048	4096	2048	2048
Tanúsítvány hash-algoritmus	SHA-256	SHA-256	SHA-256	SHA-256	SHA-256	SHA-256
Megbízható CA	igen	igen	igen	igen	igen	igen
Extended validation	nem	nem	nem	nem	igen	nem
TLS verzió	1.0	1.0,1.1,1.2	1.0	1.2	1.2	1.0,1.1,1.2
Kulcscsere algoritmus	RSA	ECDHE, RSA	RSA	ECDHE, DHE	ECDHE	ECDHE, DHE,RSA
Szimetrikus kulcs [bit]	112, 128, 256	112, 128, 256	112, 128, 256	128, 256	128, 256	128, 256
Blokkrejtjelzési üzemmód	CBC	CBC	CBC	CBC, GCM	CBC, GCM	CBC, GCM
RC4 támogatás	nem	IGEN	nem	nem	nem	nem
3DES támogatás	igen	igen	igen	nem	nem	igen
Forward Secrecy	nem	részben	nem	igen	igen	részben
HTTP Strict Transport Security	nem	nem	nem	igen	igen	nem
Összesített eredmény	C	B	C	A+	A	A

2. táblázat: a tesztek eredményeinek összehasonlítása (saját szerkesztés)

[8] Ábra forrása: Qualys SSL Labs
https://www.ssllabs.com/ssltest/analyze.html?d=www.fuehrungszeugnis.bund.de&hideResults=on
[2017. 02. 25.]

A nem megfelelő protokollok, algoritmusok és paraméterek alkalmazása lehetővé teszi a honlapok vagy a kommunikációs csatorna elleni támadást, például az utóbbi pár évben nyilvánosságra került, TLS protokoll gyengeségeit kiaknázó sebezhetőségekkel. Tekintettel arra, hogy az elavult titkosítás alkalmazása közvetlen veszélyt jelent az állampolgári adatokra, haladéktalanul szükséges ezeknek cseréje a korszerű megoldásokra. A vizsgált német elektronikus közigazgatási szolgáltatások mindegyike szinte teljes mértékben megfelel a kor biztonsági követelményeinek. Azok alkalmazása, legalábbis technológiai szempontból az állampolgárok adataira nem jelent veszélyt, de itt is javasolt a TLS 1.0 és 1.1 letiltása. Külön kiemelendő a kizárólagos tudásalapú azonosítás helyett a birtoklás és tudás alapú többfaktoros azonosítás alkalmazása. Ez kiemelten magas biztonságot tesz lehetővé, de sajnos jelentősen korlátozza az e-közigazgatási funkciók széles körben történő hozzáférését. Megoldást jelenthetne erre az Észtországban alkalmazott elektronikus „állampolgársági" kártya bevezetése, ami külföldiek számára is hozzáférhető és az e-közszolgáltatások szinte teljes köréhez teljes körű hozzáférést biztosít. [8] Javasolt e-kormányzati szolgáltatásokban a nemzetközi jó gyakorlatnak megfelelő szabványok és ajánlások használata. Így például a NIST és ETSI szabványok használata.

FELHASZNÁLT IRODALOM

[1] SZÁDECZKY T.: *Kriptográfiai protokollok megfelelősége*, Hadmérnök XI. évf. 4. sz. 2016. december. ISSN 1788-1919 pp. 178-183.

[2] LAPOSA T.: *E-közigazgatási rendszerek interoperabilitásának érettsége*, Hadmérnök XII. évf. 1. sz. 2017. március. ISSN 1788-1919 pp. 233-246.

[3] HAWANNA, V.; KULKARNI,V.Y., RANE, R.A., MESTRI, P., PANCHAL, S.: *Risk Rating System of X.509 Certificates*, Procedia Computer Science, Volume 89, 2016, Pages 152-161

[4] GASTERMANN, B.; STOPPER, M.; KOSSIK, A.; KATALINIC, B.: *Secure Implementation of an On-Premises Cloud Storage Service for Small and Medium-Sized Enterprises*, Annals of DAAAM & Proceedings. 2014, Vol. 25 Issue 1, p. 581 DOI: 10.1016/j.proeng.2015.01.407.

[5] GUERON, S., KOUNAVIS, M.: *Efficient implementation of the Galois Counter Mode using a carry-less multiplier and a fast reduction algorithm*, Information Processing Letters, Volume 110, Issues 14–15, 1 July 2010, Page 549 DOI: 10.1016/j.ipl.2010.04.011

[6] KORAY EMRE, K.; EMIN İSLAM T.: *Analysis of HTTP Security Headers in Turkey*, International Journal of Information Security Science, Dec2016, Vol. 5 Issue 4, p. 99.

[7] SLEEVI R.: *Intent to Deprecate and Remove: Trust in existing Symantec-issued Certificates*, https://groups.google.com/a/chromium.org/forum/#!topic/blink-dev/eUAKwjihhBs%5B1-25%5D [2017.04.12.]

[8] SÄRAV, S., KERIKMÄE, T., KASPER, Á.: *Az e-polgárság, mint a virtuális migráció eszköze Észtországban (The means of virtual migration - e-residency in e-Estonia),* Információs Társadalom. 2016, Vol. 16 Issue 2, p8-31. 24p.