HTTPS

DAVID BRONIEK

BRO0100

Co je to HTTPS?

Hypertext Transfer Protocol Secure

Využívá protokol TLS

Umožňuje zabezpečit spojení mezi prohlížečem a webovým serverem

Zajišťuje autentizaci, důvěrnost a integritu přenášených dat

Důvody pro nasazení HTTPS

Jistota, že komunikuji s tím, s kým opravdu chci

Ochrana uživatelů před odposlechnutím komunikace

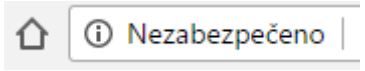
Zamezení možnosti modifikace obsahu komunikace

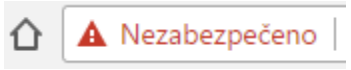
- Vložení reklamy (bezplatná Wi-Fi)
- Vložení skriptu (např. pro získání osobních údajů)

Možnost nasazení HTTP/2

Důvody pro nasazení HTTPS

Upozornění v prohlížeči na nezabezpečený web





Certifikační autorita

Jak zjistit, zda veřejný klíč služby skutečně patří této službě?

Důvěryhodný prostředník

- Ověří žadatele
- Vystaví certifikát

Úrovně ověření

DV - Domain validation

OV - Organization validation

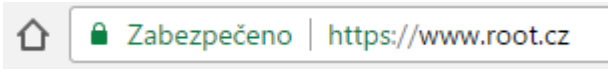
EV - Extended validation

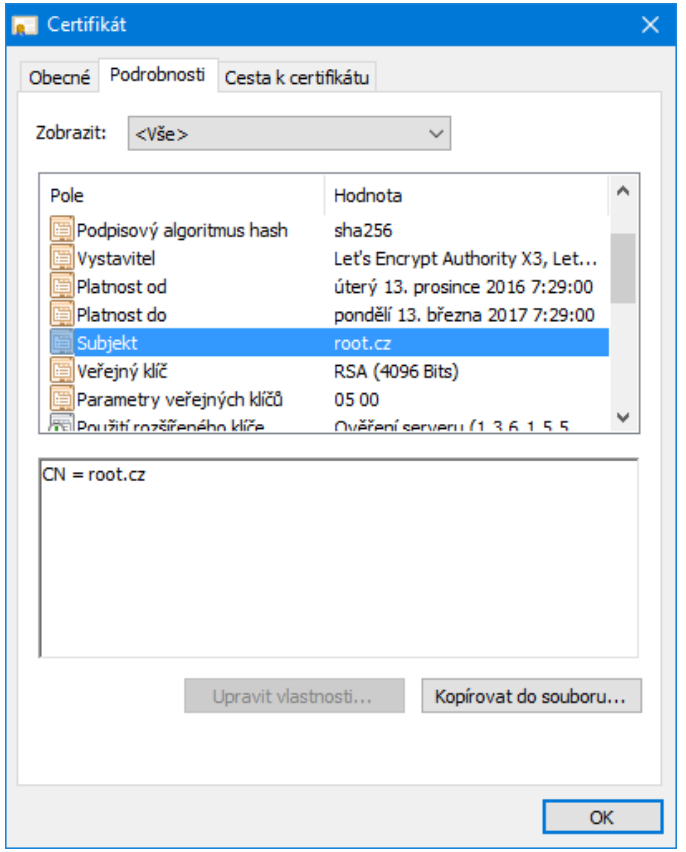
DV - Domain validation

Nejnižší úroveň ověření

Ověření domény probíhá e-mailem, existujícím souborem, DNS záznamem nebo meta tagem v HTML

Rychlé vystavení (v řádu minut)





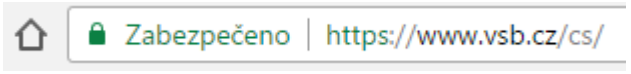
OV - Organization validation

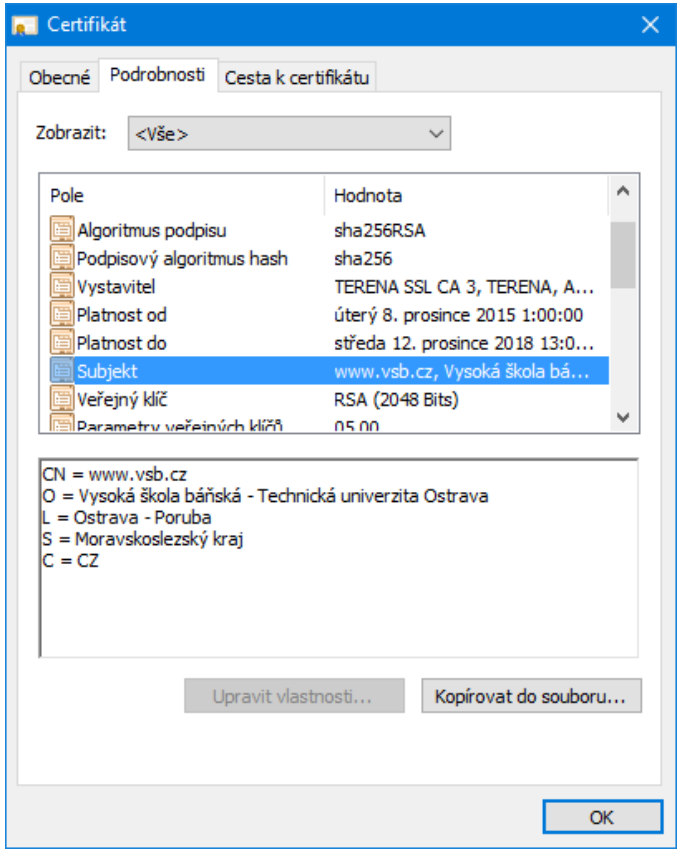
Ověření vlastníka domény – organizace

Ověření organizace trvá několik pracovních dnů

- Provádí se ověření údajů v obchodním rejstříku a telefonické ověření

V detailu certifikátu jsou uvedeny informace o organizaci

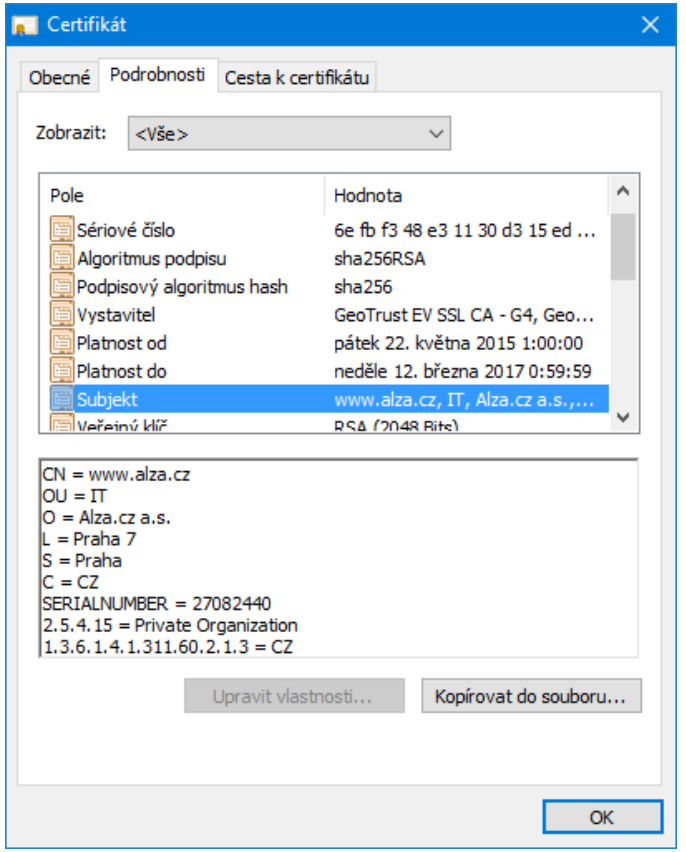




EV - Extended validation

Název organizace je uveden přímo v zeleném řádku – na první pohled zřejmý vlastník certifikátů

Důkladnější proces ověřování



Postup

Vygenerování klíčů a žádosti

Výběr certifikační autority a nutnost platit za certifikát

Instalace certifikátu a konfigurace

Hlídat se konec platnosti

Nutnost opakovat tento postup jednou za 1 až 3 roky (podle doby platnosti certifikátu)

Certifikační autorita (CA)

Společný projekt Mozilla Corporation, Cisco Systems, Akamai Technologies, Electronic Frontier Foundation (EFF), IdenTrust a University of Michigan

Představen v listopadu 2014, veřejná beta od prosince 2015, od dubna 2016 běžný provoz

Dnes několik desítek partnerů

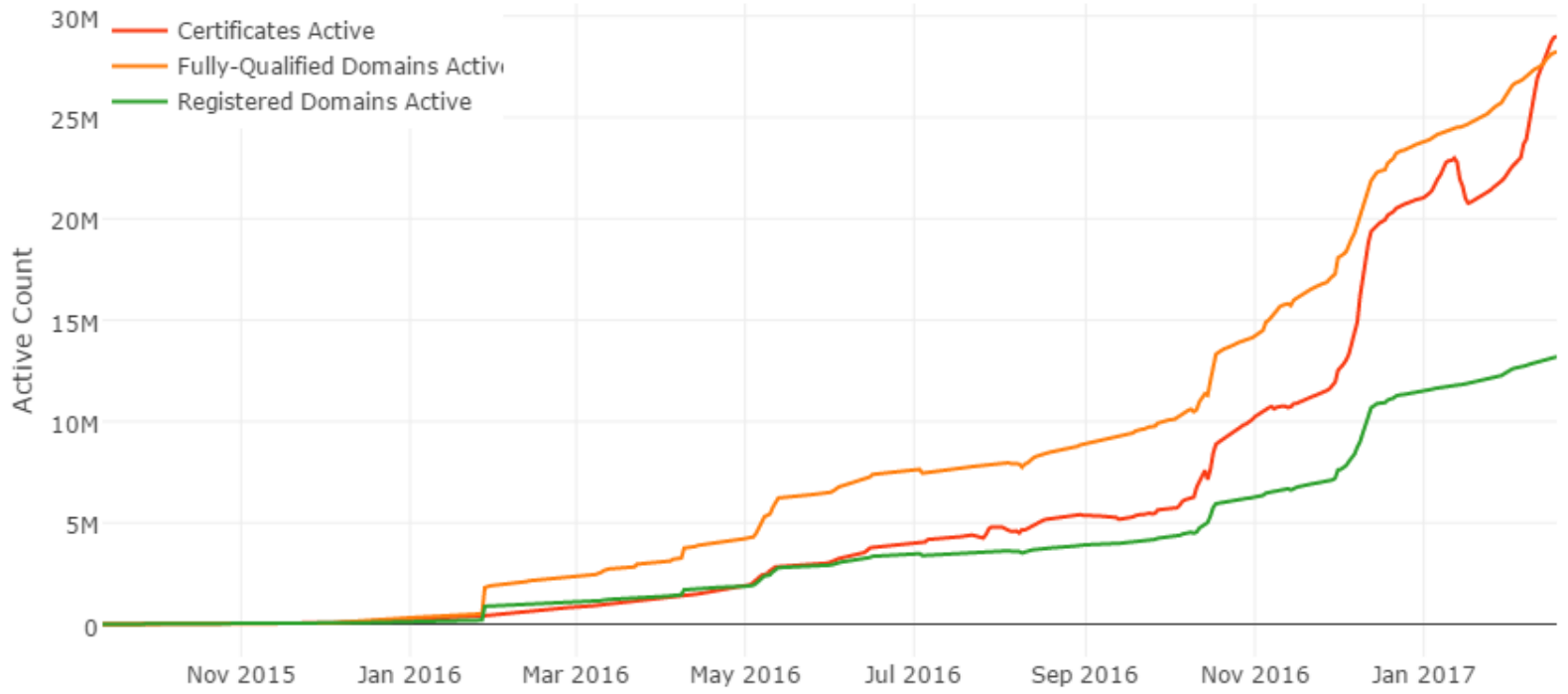
Klíčové principy

- Zdarma
- Automatizovaně
- Bezpečně
- Průhledně
- Otevřeně

Vlastnosti certifikátů

- Vystavují pouze DV certifikáty
- Nevystavují wildcard - **.example.cz*
- Vystavený certifikát je platný 3 měsíce
- Podpora SAN (Subject Alternative Name) umožňující vložit více různých doménových jmen do jednoho certifikátu - až 100 jmen v certifikátu
- Možnost kdykoliv obnovit
- Možnost revokace (zneplatnění)
- Podporuje IDN (domény s diakritikou)

Let's Encrypt



19.02.2017 - https://letsencrypt.org/stats/

Protokol ACME

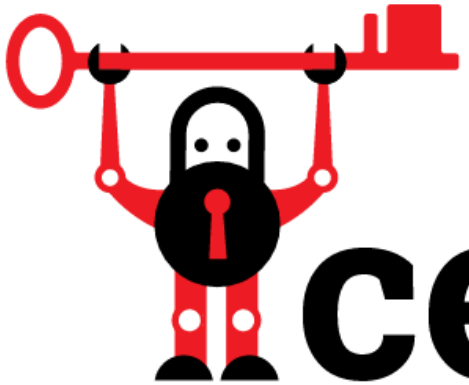
Automatic Certificate Management Environment

Navržen pro automatizaci postupu vydávání certifikátů

Komunikace stroj - stroj

Klienti:

- Certbot – oficiální klient, maximalně automatizován
- acme.sh – klient napsaný v shellu
- https://gethttpsforfree.com – webový klient
- Několik desítek dalších klientů – https://letsencrypt.org/docs/client-options/



certbot

Automatically enable HTTPS on your website with EFF's Certbot, deploying Let's Encrypt certificates.

I'm using Apache on Ubuntu 16.04 (xenial)

Apache on Ubuntu 16.04 (xenial)

automated | advanced

Install

Since Certbot is packaged for your system, all you'll need to do is apt-get the following packages.

```
$ sudo apt-get install python-letsencrypt-apache
```

Get Started

Certbot has a fairly solid beta-quality Apache plugin, which is supported on many platforms, and automates both obtaining and installing certs:

```
$ letsencrypt --apache
```

SSL Labs - Server Test

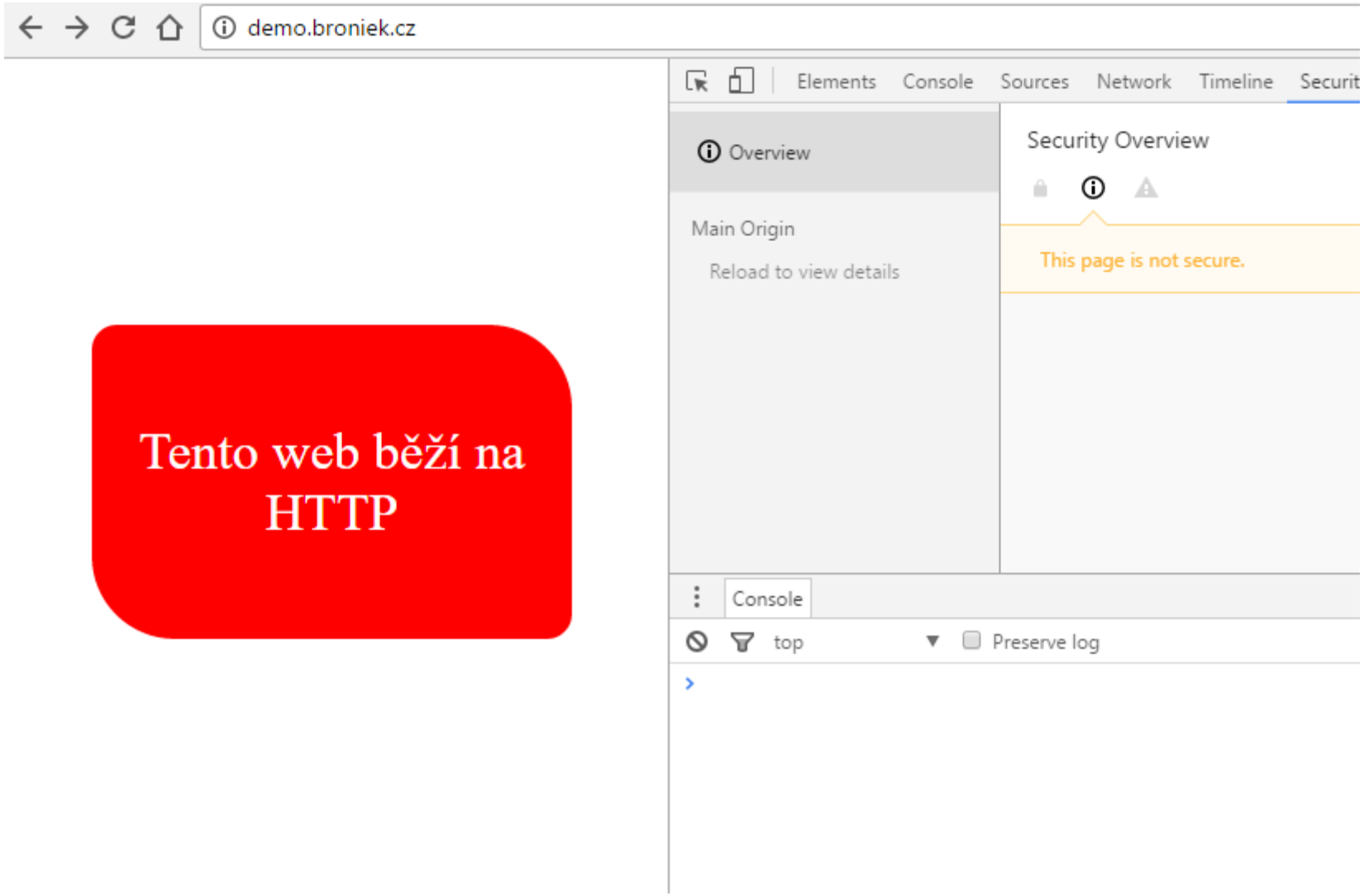
Online služba umožňující otestovat webový server (https://www.ssllabs.com)

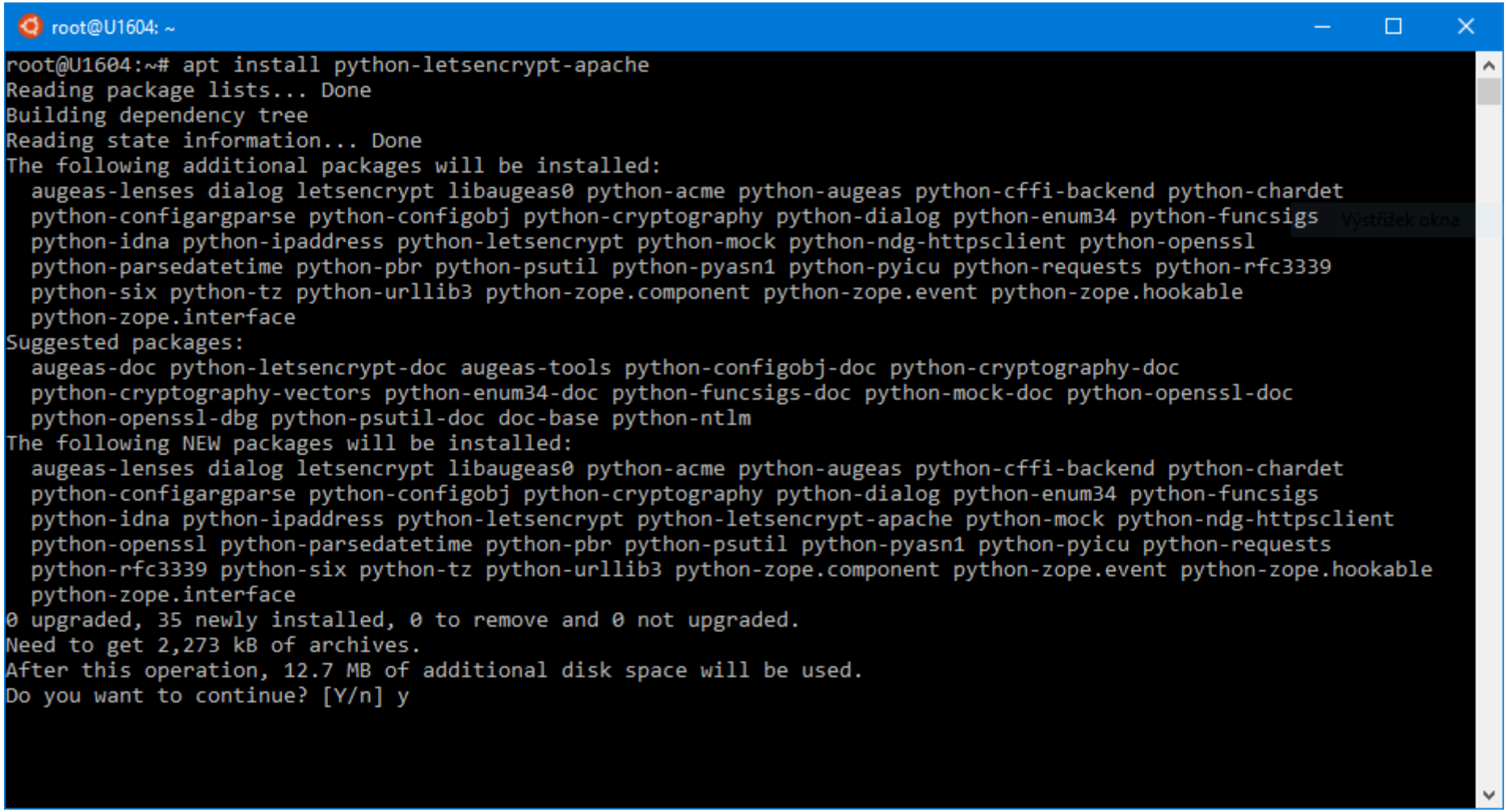
Bezpečnost ohodnotí známkou

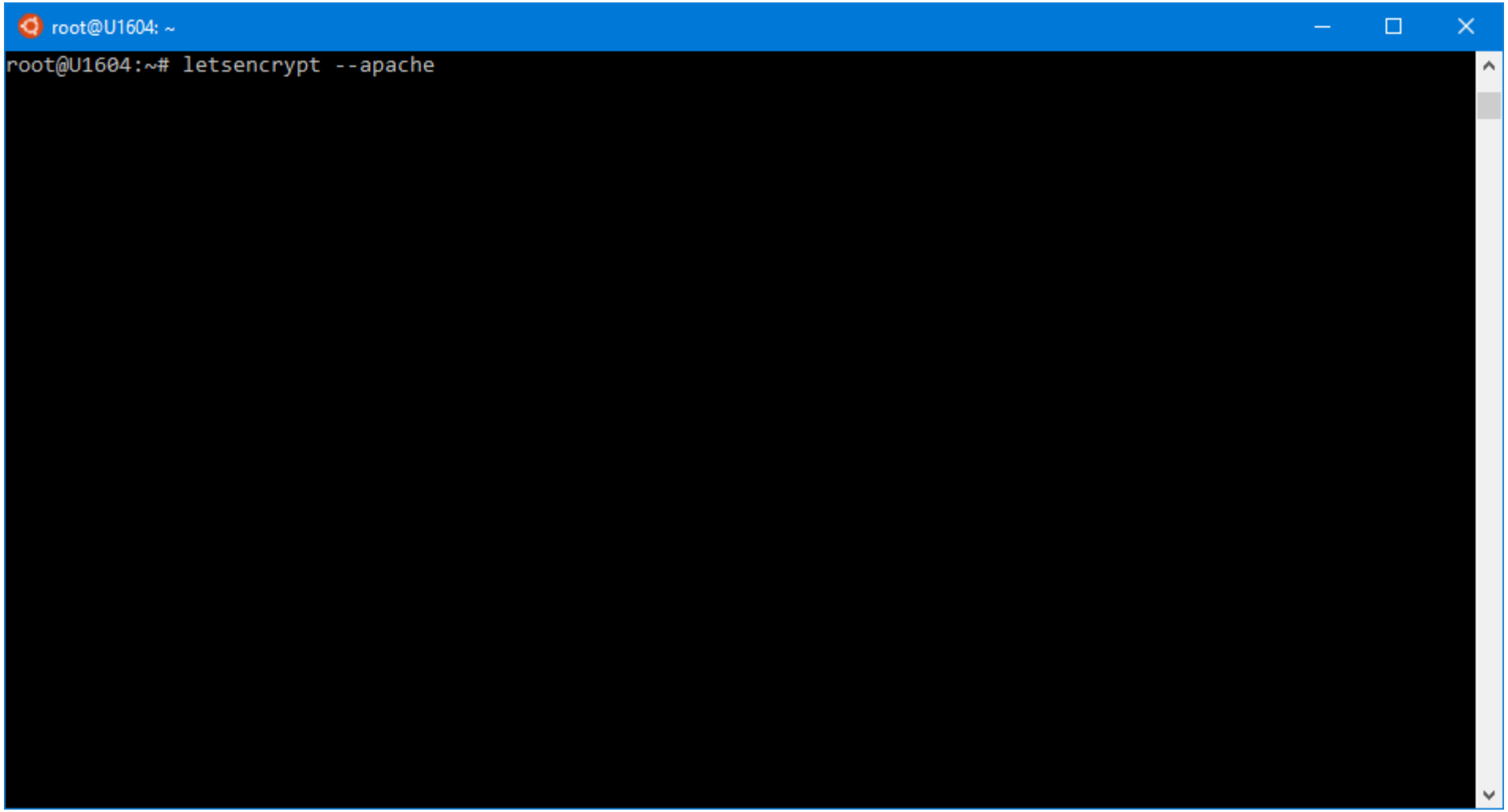
Podrobné výsledky (povolené protokoly a šifry, otestování zranitelností, informace o certifikátu, …)

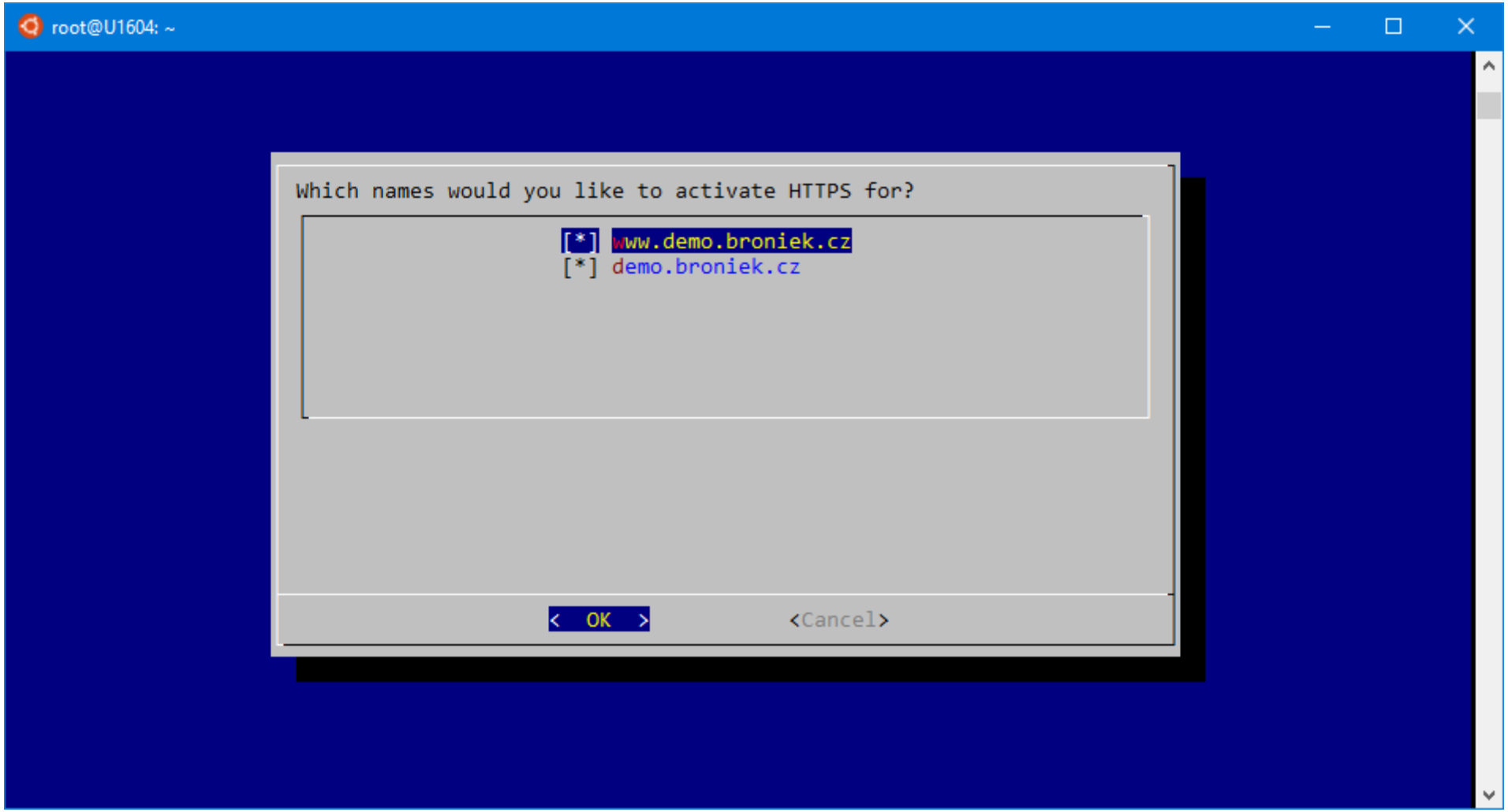
Ukázka

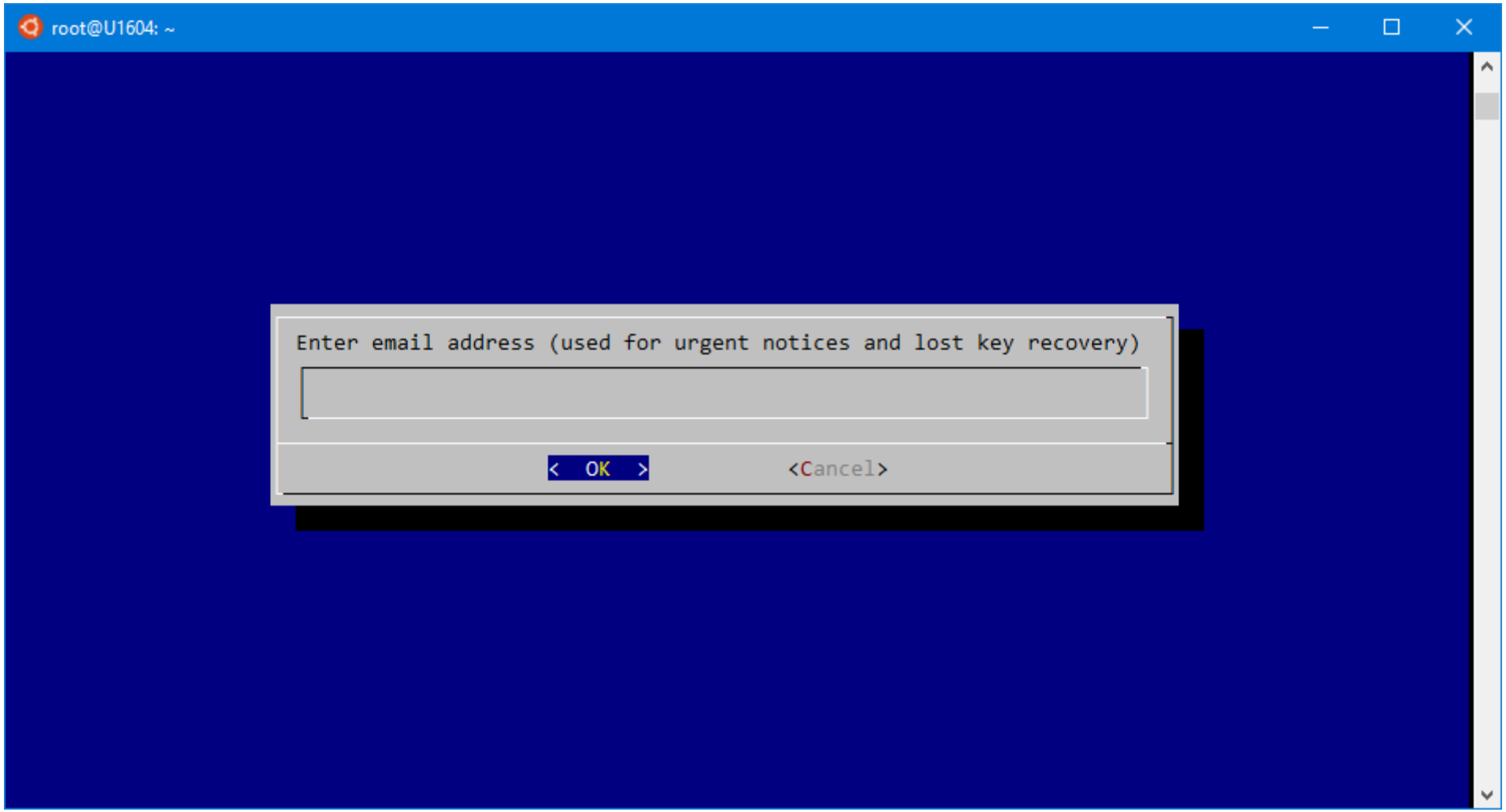
NASAZENÍ HTTPS OD LET'S ENCRYPT NA WEB SERVER APACHE

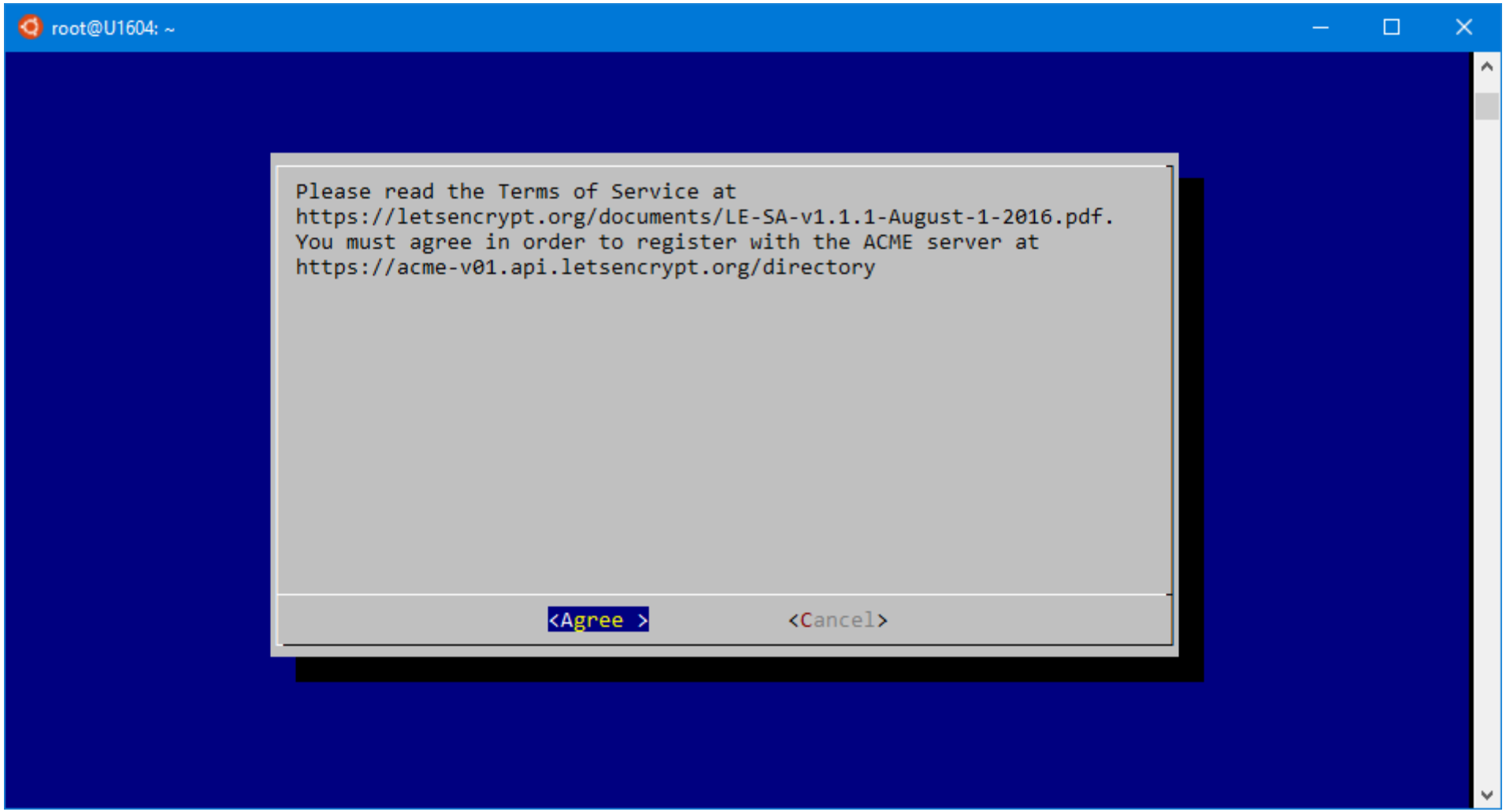

demo.broniek.cz
Elements
Console
Sources
Network
Timeline
Securit
Overview
Main Origin
Reload to view details
Security Overview
This page is not secure.
Console
top
Preserve log
Tento web běží na HTTP

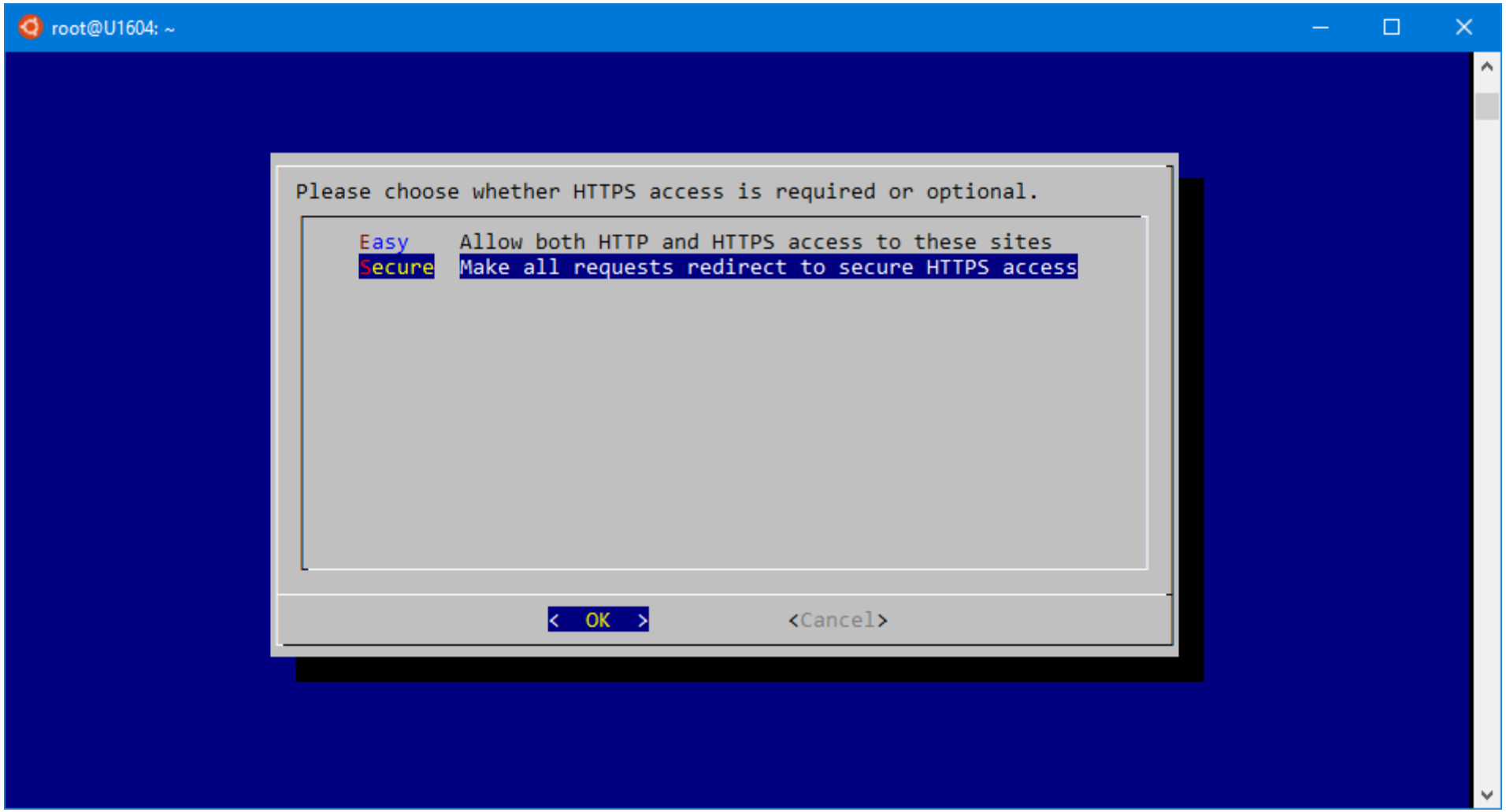

root@U1604: ~
root@U1604:~# apt install python-letsencrypt-apache
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
augeas-lenses dialog letsencrypt libaugeas0 python-acme python-augeas python-cffi-backend python-chardet
python-configargparse python-configobj python-cryptography python-dialog python-enum34 python-funcsigs
python-idna python-ipaddress python-letsencrypt python-mock python-ndg-httpsclient python-openssl
python-parsedatetime python-pbr python-psutil python-pyasn1 python-pyicu python-requests python-rfc3339
python-six python-tz python-urllib3 python-zope.component python-zope.event python-zope.hookable
python-zope.interface
Suggested packages:
augeas-doc python-letsencrypt-doc augeas-tools python-configobj-doc python-cryptography-doc
python-cryptography-vectors python-enum34-doc python-funcsigs-doc python-mock-doc python-openssl-doc
python-openssl-dbg python-psutil-doc doc-base python-ntlm
The following NEW packages will be installed:
augeas-lenses dialog letsencrypt libaugeas0 python-acme python-augeas python-cffi-backend python-chardet
python-configargparse python-configobj python-cryptography python-dialog python-enum34 python-funcsigs
python-idna python-ipaddress python-letsencrypt python-letsencrypt-apache python-mock python-ndg-httpsclient
python-openssl python-parsedatetime python-pbr python-psutil python-pyasn1 python-pyicu python-requests
python-rfc3339 python-six python-tz python-urllib3 python-zope.component python-zope.event python-zope.hookable
python-zope.interface
0 upgraded, 35 newly installed, 0 to remove and 0 not upgraded.
Need to get 2,273 kB of archives.
After this operation, 12.7 MB of additional disk space will be used.
Do you want to continue? [Y/n] y

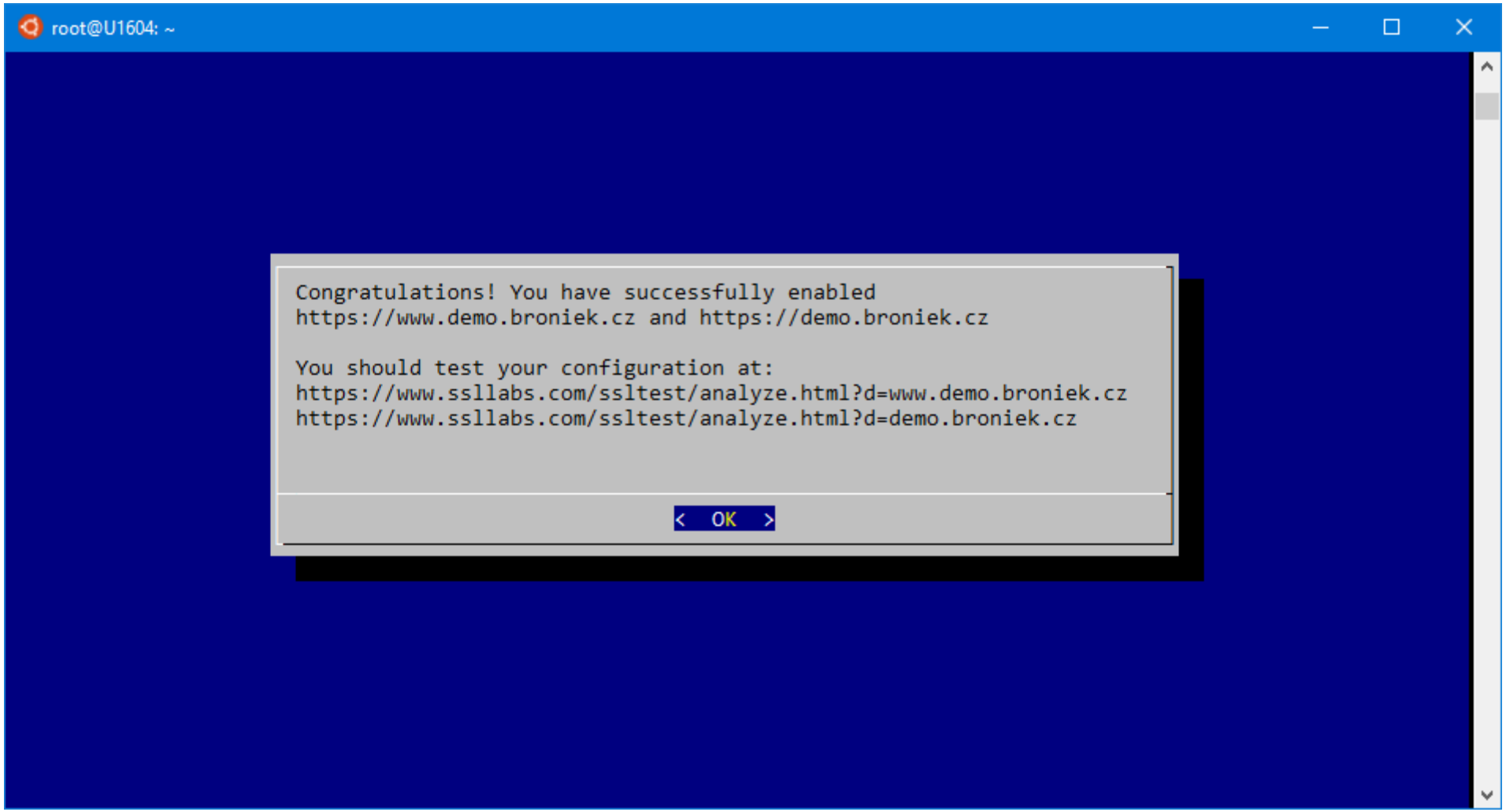

root@U1604: ~
root@U1604:~# letsencrypt --apache

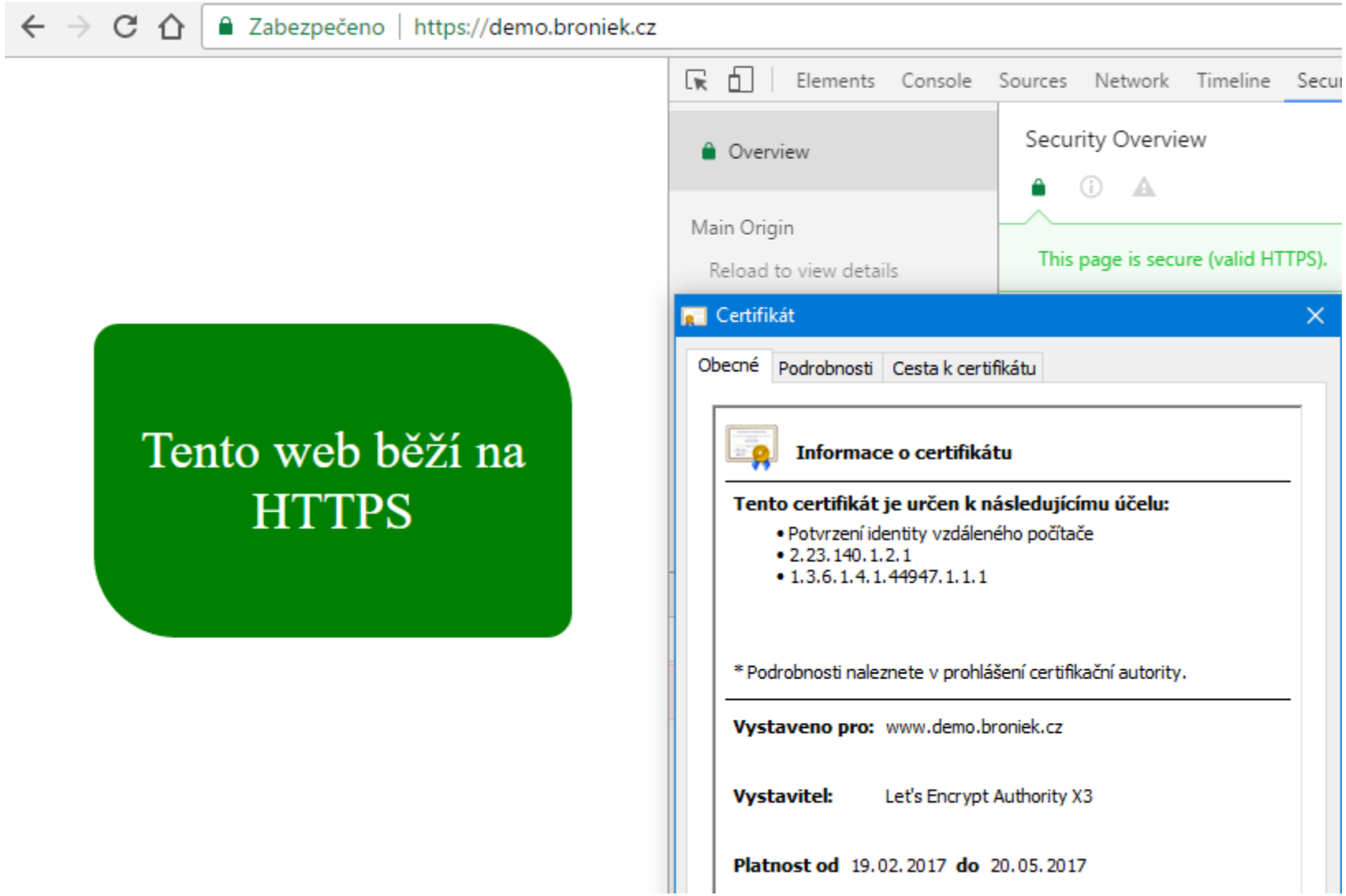

root@U1604: ~
Which names would you like to activate HTTPS for?
[*] www.demo.broniek.cz
[*] demo.broniek.cz
< OK >
<Cancel>


root@U1604: ~
Enter email address (used for urgent notices and lost key recovery)
< OK >
<Cancel>

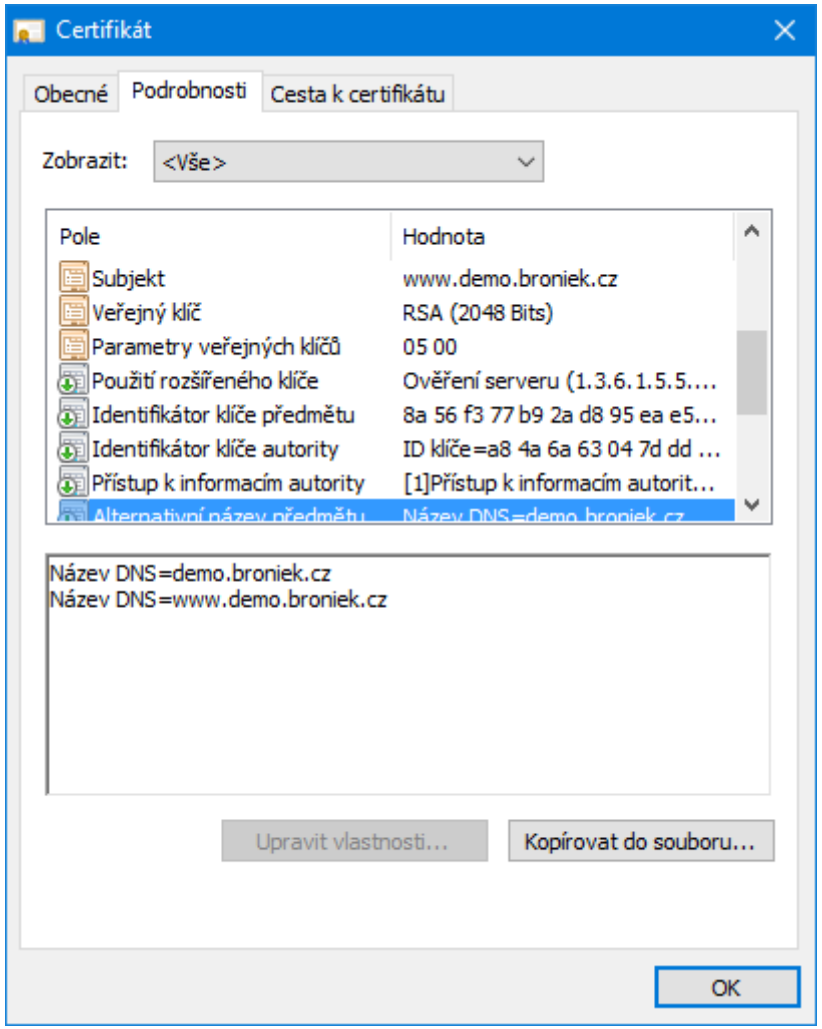

root@U1604: ~
Please read the Terms of Service at
https://letsencrypt.org/documents/LE-SA-v1.1.1-August-1-2016.pdf.
You must agree in order to register with the ACME server at
https://acme-v01.api.letsencrypt.org/directory
<Agree >
<Cancel>


root@U1604: ~
Please choose whether HTTPS access is required or optional.
Easy Allow both HTTP and HTTPS access to these sites
Secure Make all requests redirect to secure HTTPS access
< OK >
<Cancel>


root@U1604: ~
Congratulations! You have successfully enabled
https://www.demo.broniek.cz and https://demo.broniek.cz
You should test your configuration at:
https://www.ssllabs.com/ssltest/analyze.html?d=www.demo.broniek.cz
https://www.ssllabs.com/ssltest/analyze.html?d=demo.broniek.cz
< OK >



Tento web běží na HTTPS


Certifikát
Obecné
Podrobnosti
Cesta k certifikátu
Zobrazit:
<Vše>
Pole
Hodnota
Subjekt
www.demo.broniek.cz
Veřejný klíč
RSA (2048 Bits)
Parametry veřejných klíčů
05 00
Použití rozšířeného klíče
Ověření serveru (1.3.6.1.5.5....
Identifikátor klíče předmětu
8a 56 f3 77 b9 2a d8 95 ea e5...
Identifikátor klíče autority
ID klíče=a8 4a 6a 63 04 7d dd ...
Přístup k informacím autority
[1]Přístup k informacím autorit...
Název DNS=demo.broniek.cz
Název DNS=www.demo.broniek.cz
Upravit vlastnosti...
Kopírovat do souboru...
OK

SSL Report: demo.broniek.cz (185.28.102.217)

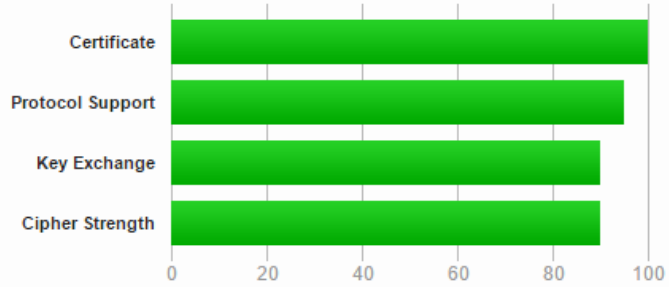
Assessed on: Sun, 19 Feb 2017 17:56:28 UTC | **HIDDEN** | Clear cache

Scan Another »

Summary

Overall Rating

A



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

Certificate #1: RSA 2048 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	www.demo.broniek.cz Fingerprint SHA1: 8f54c64f5158b5f81c2f8a0c5ec7ad1a7ba4215d Pin SHA256: gvFRaVtVPIaDHbSIJkug+FeXIuPHaqkIQoMCyyQscKA=
Common names	www.demo.broniek.cz
Alternative names	demo.broniek.cz www.demo.broniek.cz
Valid from	Sun, 19 Feb 2017 16:46:00 UTC
Valid until	Sat, 20 May 2017 16:46:00 UTC (expires in 3 months)
Key	RSA 2048 bits (e 65537)

HSTS

HTTP Strict Transport Security

Hlavička v HTTP odpovědi

Trust On First Use (TOFU)

Prohlížeč bude vědět, že všechny další požadavky k tomuto serveru mají jít výhradně prostřednictvím HTTPS

Web musí mít vždy důvěryhodný certifikát

Obrana proti útoku SSL Strip

Známka A+ ve https://www.ssllabs.com

```
Strict-Transport-Security: max-age=31536000; includeSubDomains
```

HSTS preload

Preload list

- Některé adresy jsou předinstalovaný ve zdrojovém kódu prohlížeče
- Žádost o přidání na adrese https://hstspreload.org/
- Vždy půjde přímo na HTTPS

```
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
```

HTTPS Everywhere

Extension pro Chrome, Firefox a Operu

Seznam webů, na které se bude rovnou posílat požadavek na HTTPS

https://www.eff.org/https-everywhere

Děkuji za pozornost

Zdroje

https://letsencrypt.org/

https://www.owasp.org/index.php/HTTP_Strict_Transport_Security_Cheat_Sheet

http://www.samuraj-cz.com/clanek/protokol-ssl-tls-slabe-sifry-zranitelnosti-a-jejich-testovani/