Role certifikátů v bezpečné komunikaci

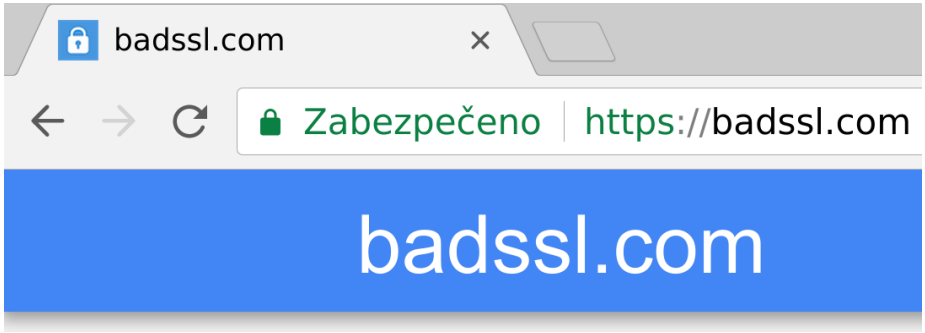
Ondřej Caletka

26. dubna 2018

Obsah

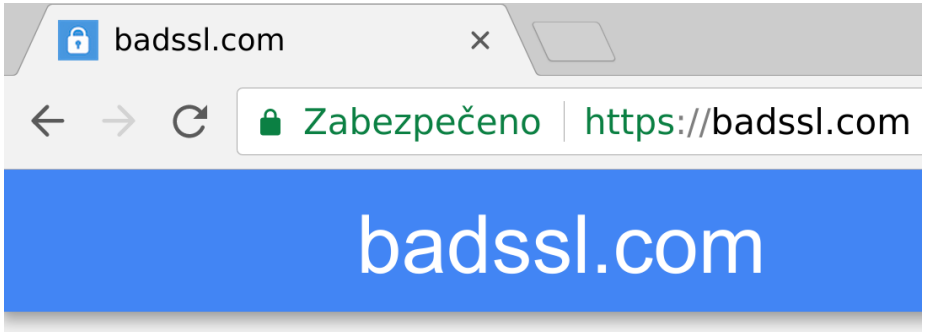
cesnet

Co znamená nápis „Zabezpečeno“?



cesnet

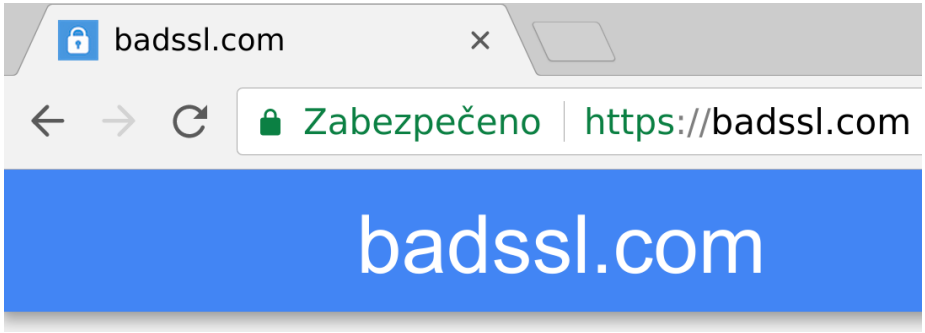
Co znamená nápis „Zabezpečeno“?



a) stránka je důvěryhodná
b) spojení se serverem je šifrováno
c) totožnost provozovatele stránky byla ověřena
d) všechny předchozí možnosti

cesnet

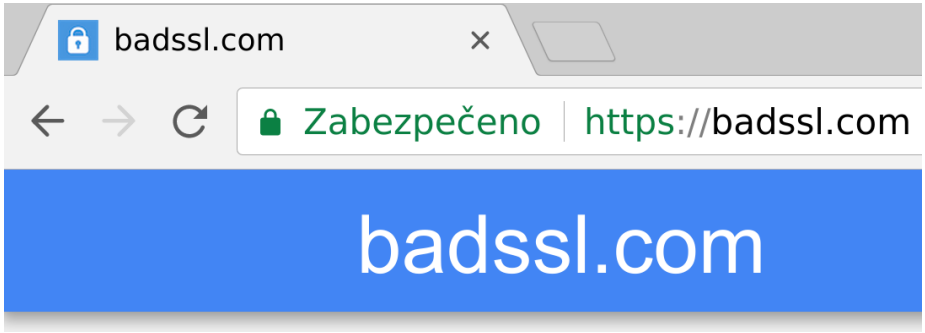
Co znamená nápis „Zabezpečeno“?



a) stránka je důvěryhodná
b) **spojení se serverem je šifrováno**
c) totožnost provozovatele stránky byla ověřena
d) všechny předchozí možnosti

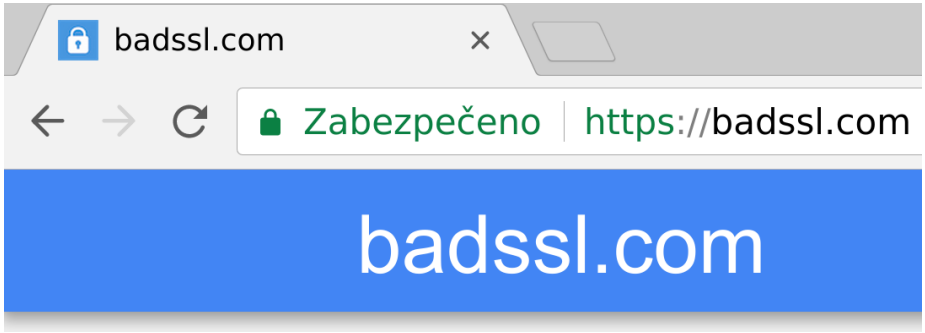
cesnet

Který výrok je pravdivý?



cesnet

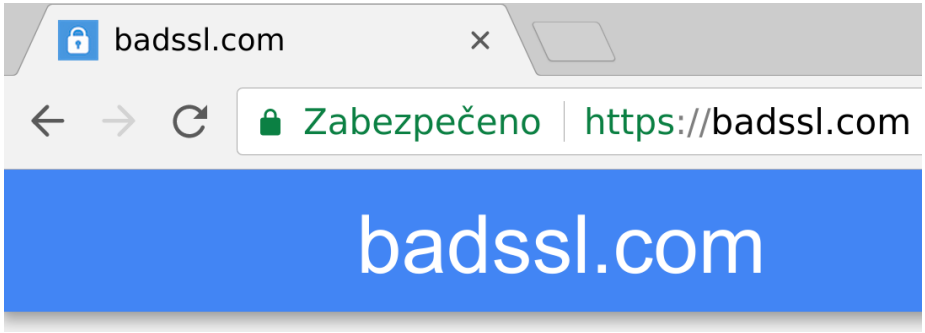
Který výrok je pravdivý?



a) certifikát slouží k šifrování
b) certifikát je potřeba chránit před odcizením
c) při použití EV certifikátu je přenos bezpečnější
d) žádný z předchozích

cesnet

Který výrok je pravdivý?



a) certifikát slouží k šifrování
b) certifikát je potřeba chránit před odcizením
c) při použití EV certifikátu je přenos bezpečnější
d) **žádný z předchozích**

cesnet

Infrastruktura veřejného klíče

- řeší problém důvěryhodného ověření identity protistrany
- **certifikát = průkaz totožnosti** vystavený důvěryhodnou autoritou
  - svazuje virtuální identitu (šifrovací klíč) s reálnou identitou (jméno a příjmení, adresa, doménové jméno,...)
  - zapečetěný elektronickým podpisem autority
- důvěryhodné autority **jsou předinstalovány v počítači**

cesnet

Pojmy z oblasti PKI ①

privátní klíč tajné číslo, umožňující rozšifrovat zprávu a vytvořit elektronický podpis

veřejný klíč číslo, umožňující zašifrovat zprávu a ověřit elektronický podpis. Lze jej vypočítat z privátního klíče

požadavek (CSR) dokument standardu PKCS#10, obsahující veřejný klíč, identifikaci subjektu a omezení využití certifikátu

certifikát podepsaný dokument standardu X.509, obsahující veřejný klíč, identifikaci subjektu a omezení využití certifikátu

cesnet

Pojmy z oblasti PKI (2)

cerifikační autorita instituce nebo software, který podepisuje požadavky a vytváří certifikáty

self-signed certifikát, jehož podpis byl vytvořen klíčem, jehož veřejnou část obsahuje

pevný bod důvěry certifikát, jehož věrohodnost byla ověřena jiným způsobem a je považován za důvěryhodný

řetěz důvěry sekvence podepsaných certifikátů od pevného bodu důvěry ke koncovému certifikátu

cesnet

Jak probíhá ověření

Cestovní pas

1. cestující předloží cestovní pas a své biometrické údaje
2. ověříme shodu biometrických údajů
3. ověříme pravost dokumentu
4. ověříme, že vydavatel je na seznamu uznávaných vydavatelů
5. známe identitu cestujícího

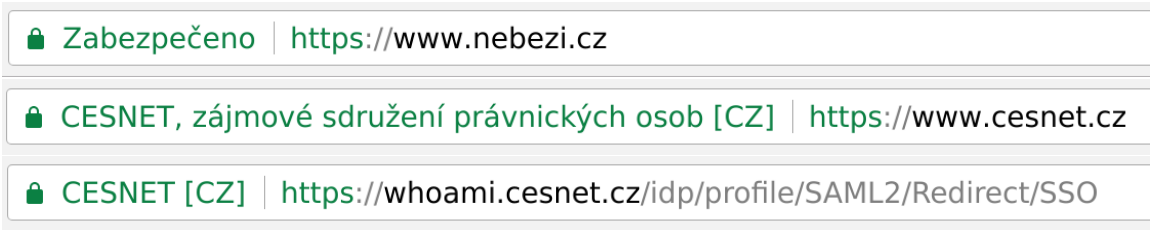
Certifikát

1. protistrana předloží certifikát a důkaz vlastnictví privátního klíče
2. ověříme důkaz vlastnictví
3. ověříme podpis certifikační autority
4. ověříme, že autorita je na seznamu důvěryhodných
5. známe identitu protistrany

cesnet

Úrovně ověření certifikátů

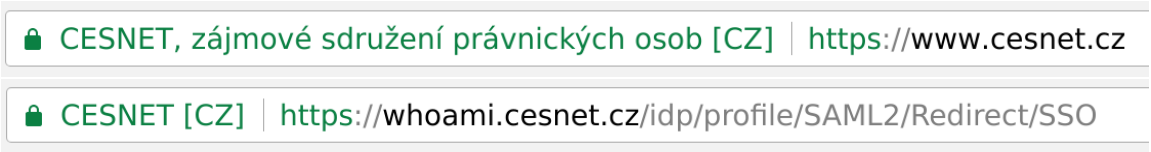
- DV ověření držení doménového jména (€)
- OV ověření totožnosti osoby (€€)
- EV důkladnější ověření totožnosti osoby (€€€)



cesnet

EV certifikáty

- autority samostatně ověřují pravost žadatele
- jméno držitele výrazně vyznačeno v prohlížečích
- platnost maximálně 2 roky (825 dnů)
- musí být zveřejněny v *Certificate Transparency*
- nelze použít *žolík*



cesnet

OV a DV certifikáty

- liší se pouze v detailech certifikátu
  - `DV` obsahuje pouze doménová jména
  - `OV` obsahuje doménová jména a jména osob
- od 1. března 2018 platnost maximálně 2 roky (825 dnů)
- od 30. dubna 2018 musí být zveřejněny v *Certificate Transparency*
- lze použít *žolík* (**ale jen v nezbytných případech**)

cesnet

Proč je žolík špatný nápad

- platí pro jakékoli doménové jméno **dané úrovně**[1]
- jeho kompromitace vede ke kompromitaci celé nadřazené domény
- na možnost revokace nelze příliš spoléhat
- na druhou stranu, jde o jedinou možnost, jak nezveřejnit doménová jména

[1] certifikát pro `*.example.com` neplatí pro `some.other.example.com`

cesnet

Proč nefunguje revokace

Certificate Revocation List

- příliš mnoho autorit
- příliš mnoho revokovaných certifikátů
- příliš časté aktualizace

Online Certificate Status Protocol

- nárok na dostupnost odpovídače
- *soft-fail* implementace nedává smysl
- vliv na soukromí

CRLSets

- seznam revokovaných certifikátů pro Chrome
- obsahuje jen *důležité* revokace
- způsob výroby neveřejný

OCSP stapling

- OCSP odpověď *připnutá* k certifikátu
- volba certifikátu `MustStaple` vyžaduje připnutí odpovědi

cesnet

- otevřená, bezplatná, plně automatická certifikační autorita
- vydává pouze DV certifikáty
- otevřený protokol ACME pro komunikaci žadatele a autority

Způsoby ověření držení domény

`http-01` vystavením souboru na autoritou určené cestě `/.well-known/acme-challenge/…`

`dns-01` vystavením DNS TXT záznamu na jméno `_acme-challenge.<vydávané jméno>`

~~`tls-sni-01` použitím TLS certifikátu vystaveného na speciální jméno~~

Je Let's Encrypt hrozbou?

- stačí chvilkové ovládnutí doménového jména
- lze selektivně odbočit provoz jen při ověřování
- problémy se sdílenými webhostingy
  - často nevalidují příslušnost domény k danému zákazníkovi
  - týká se i velkých cloudových služeb

cesnet

Skutečnou hrozbou jsou DV certifikáty

- stejný princip fungoval i před Let's Encrypt a funguje stále
- nejčastější způsoby validace držení domény
  - příjem e-mailu na dané doméně
  - vystavení souboru na webserveru
  - vystavení TXT záznamu v DNS
- cena několika stokorun útočníka neodradí

Scott Helme: We need more phishing sites on HTTPS!

Trusted Certificate Service

- služba panevropského akademického sdružení GÉANT
- možnost získat důvěryhodné OV a EV certifikáty od autority Digicert
- platnost certifikátů až dva roky
- ruční validace e-mailem jednou za čas
- k dispozici **zdarma** pro všechny klienty e-infrastruktury CESNET

cesnet

DNS záznam typu CAA

- určuje autority, které jsou oprávněny vydat certifikát na dané jméno[2]
- kontrolován autoritami povinně od září 2017
- postupná kontrola od daného jména směrem k TLD
  - lze nastavit obecnou politiku domény a výjimky pro jednotlivé subdomény
- samostatné určení pro standardní a *žolíkové* certifikáty
- granularita (*prozatím*) pouze na úrovni certifikačních autorit

Příklad

```
cesnet-ca.cz. IN CAA 0 issue "digicert.com"
cesnet-ca.cz. IN CAA 0 issuewild ";"
```

[2] jde však pouze o organizační, nikoli technické opatření

Certificate Transparency

- něco jako *registr smluv*
- certifikát, který nebyl zveřejněn, neplatí
- robustní – nevyžaduje online kontroly
  - s certifikátem musí být doručen i důkaz existence v důvěryhodném logu
- možnost kontrolovat vydané certifikáty pro danou doménu
  - crt.sh
  - Cert Spotter
  - Facebook CT monitor
- prozrazuje doménová jména (*teoreticky nemusí*)
- závisí na bezplatných službách třetích stran

cesnet

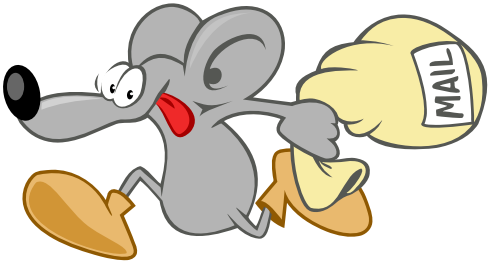
Kontrola funkčnosti certifikátů

- Nagios / Icinga
  - hlídání konce platnosti
  - hlídání úplnosti cesty důvěry
  - kontrola revokace certifikátu
- Cert Spotter
  - hlídání neoprávněného vystavení certifikátu na naše doménová jména
- On-line kontrola Qualys SSL Labs

cesnet

Smutný příběh DANE

- eliminuje roli certifikačních autorit ve vydávání DV certifikátů
- ověření držení domény se provádí při každém použití certifikátu
- starší než CAA a Let's Encrypt, přesto ignorováno webovou komunitou
- **jediné funkční řešení** pro bezpečné předávání pošty



Root.cz: Bezpečnější předávání pošty s TLSA záznamy

cesnet

Závěrečné shrnutí

- správný certifikát není všechno
  - je nutné zakázat **zastaralé šifry**[3]
  - server musí posílat **úplnou cestu**
  - kontrola webovým prohlížečem **nestačí**
- žolíkové certifikáty jen v nezbytných případech, nejlépe s `MustStaple`[4]
- pomocí CAA lze *zablokovat* cizí autority
- nezveřejněné certifikáty neplatí
- EV certifikáty jsou bezpečnější, díky TCS je lze získat **zdarma**
- pro bezpečné předávání pošty je nezbytný DNSSEC a DANE

[3] Mozilla SSL Configuration Generator
[4] Scott Helme: OCSP Must-Staple

cesnet

Děkuji za pozornost

Ondřej Caletka
Ondrej.Caletka@cesnet.cz
https://**Ondřej.Caletka.cz**

Prezentace je již nyní k dispozici ke stažení.