

Role certifikátů v bezpečné komunikaci

Ondřej Caletka



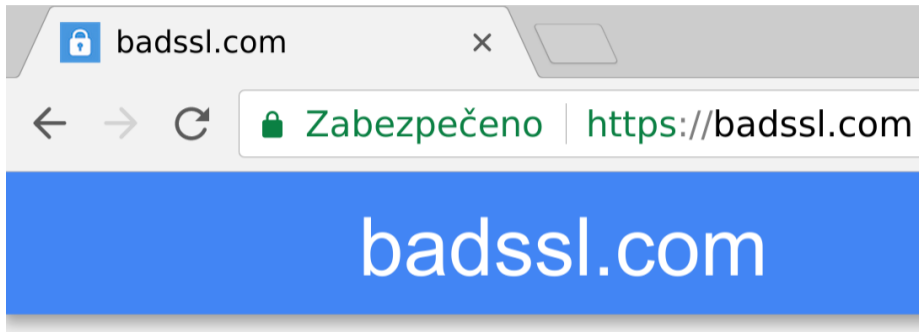
6. února 2018



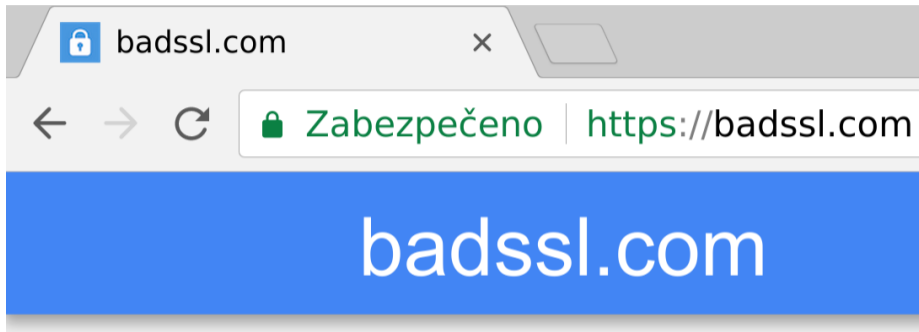
Uvedené dílo podléhá licenci Creative Commons Uveďte autora 3.0 Česko.

- 1 Kvíz
- 2 Letmý úvod do TLS a PKI
- 3 Praktická doporučení

Co znamená nápis „Zabezpečeno“?

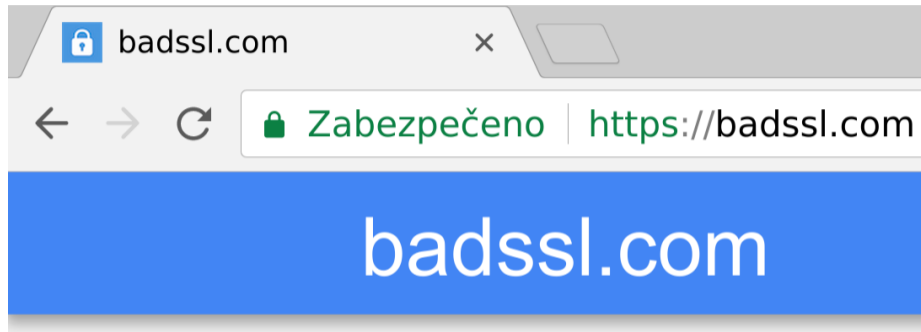


Co znamená nápis „Zabezpečeno“?



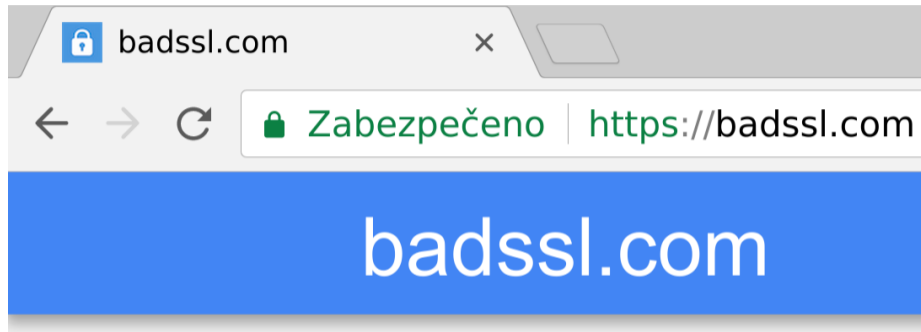
- a) stránka je důvěryhodná
- b) spojení se serverem je šifrováno
- c) totožnost provozovatele stránky byla ověřena
- d) všechny předchozí možnosti

Co znamená nápis „Zabezpečeno“?

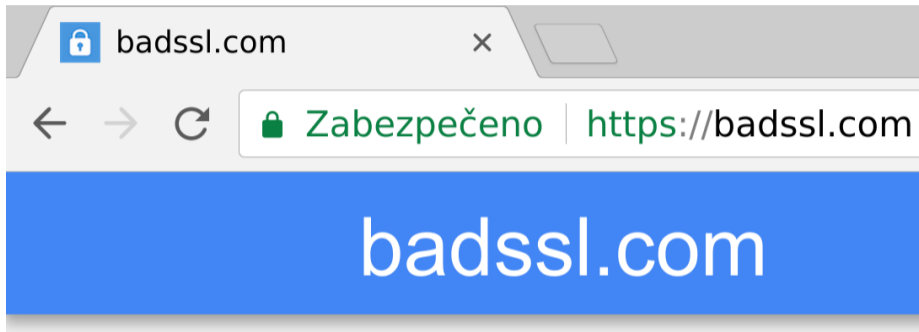


- a) stránka je důvěryhodná
- b) **spojení se serverem je šifrováno**
- c) totožnost provozovatele stránky byla ověřena
- d) všechny předchozí možnosti

Který výrok je pravdivý?

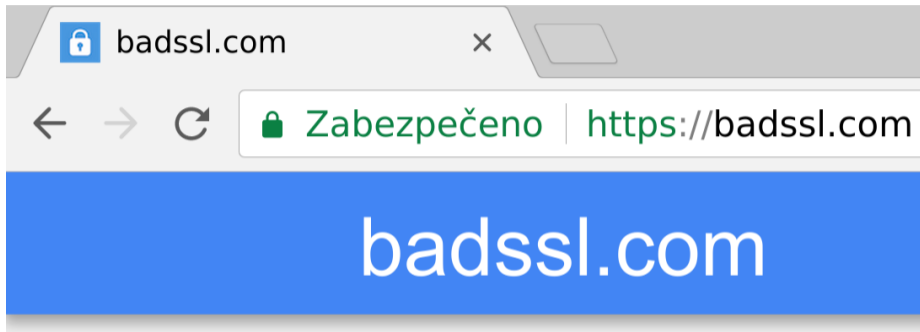


Který výrok je pravdivý?



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

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**

- 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**

- 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

certifikační 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

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

Úrovně ověření certifikátů

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

 Zabezpečeno | <https://www.nebezi.cz>

 CESNET, zájmové sdružení právnických osob [CZ] | <https://www.cesnet.cz>

 CESNET [CZ] | <https://whoami.cesnet.cz/idp/profile/SAML2/Redirect/SSO>

EV certifikáty

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

🔒 CESNET, zájmové sdružení právnických osob [CZ] | <https://www.cesnet.cz>

🔒 CESNET [CZ] | <https://whoami.cesnet.cz/idp/profile/SAML2/Redirect/SSO>

- liší se pouze v detailech certifikátu
 - DV obsahuje pouze doménová jména
 - OV obsahuje doménová jména a jména osob
- platnost maximálně 3 roky (**do konce února 2018**)
- nemusí být zveřejněny v *Certificate Transparency* (**do konce března 2018**)
- lze použít žolík (**ale jen v nezbytných případech**)

 Zabezpečeno | <https://www.nebezi.cz>

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



¹certifikát pro *.example.com neplatí pro some.other.example.com

Proč nefunguje revokace

Certificate Revocation List

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

CRLSets

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

Online Certificate Status Protocol

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

OCSP stapling

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



Let's Encrypt

- 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

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
- lze vybrat autoritu, která (*prozatím*) nezveřejňuje vydané certifikáty

Scott Helme: We need more phishing sites on HTTPS!

DNS záznam typu CAA

- určuje authority, které jsou oprávněny vydat certifikát na dané jméno²
- 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

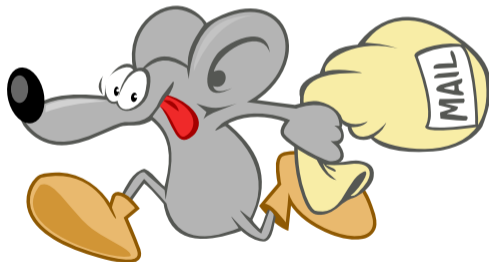
```
cesnet-ca.cz. IN CAA 0 issue "digicert.com"  
cesnet-ca.cz. IN CAA 0 issuewild ";"
```

²jde však pouze o organizační, nikoli technické opatření

- 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
 - Certspotter
 - Facebook CT monitor
- prozrazuje doménová jména (*teoreticky nemusí*)
- závisí na bezplatných službách třetích stran

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

- poslední šance **získat certifikát na 3 roky**
- nezveřejněné certifikáty neplatí
- žolíkové certifikáty jen v nezbytných případech, vždy s volbou MustStaple
- pomocí CAA lze *zablokovat* cizí autority

Děkuji za pozornost

Ondřej Caletka
Ondrej.Caletka@cesnet.cz
[https://Ondřej.Caletka.cz](https://Ondrej.Caletka.cz)

