Riscos com

Certificados internos e novos gTLDs

Rubens Kühl (GTS-21 Foz do Iguaçu, 05/2013)
Warren Kumari (ICANN Beijing, 2013-04)

TLDs: Definição e uso

- *DNS: TLDs, gTLDs e ccTLDs*
- *RFCs -> IANA -> ICANN*
- *Novos gTLDs (2000, 2003-4, 2012)*

O que vem por aí

- *Alguns possíveis novos gTLDs (http://newgtlds.icann.org)*
  - *.bom, .final, .web, .ninja, .secure*
  - *.itau, .bradesco, .amazon, .patagonia*
  - *.corp, .ads, .home, .site, .office*

Certificados

- *Uma chave pública é exigida para https:// ; ela é transportada num certificado.*
- *Que é obtido de uma Autoridade Certificadora*
- *Liga a chave pública à identidade*
- *Usado pelo browser para se certificar de estar falando com o servidor coreto*

Validação

- *Validação* é feita enviando um token para um endereço de e-mail (webmaster@ ou contato do WHOIS)
- Responder com o token prova "propriedade" do domínio.

* : Certificados do tipo DV - "Domain Validated". EV / OV tem validações mais abrangentes.

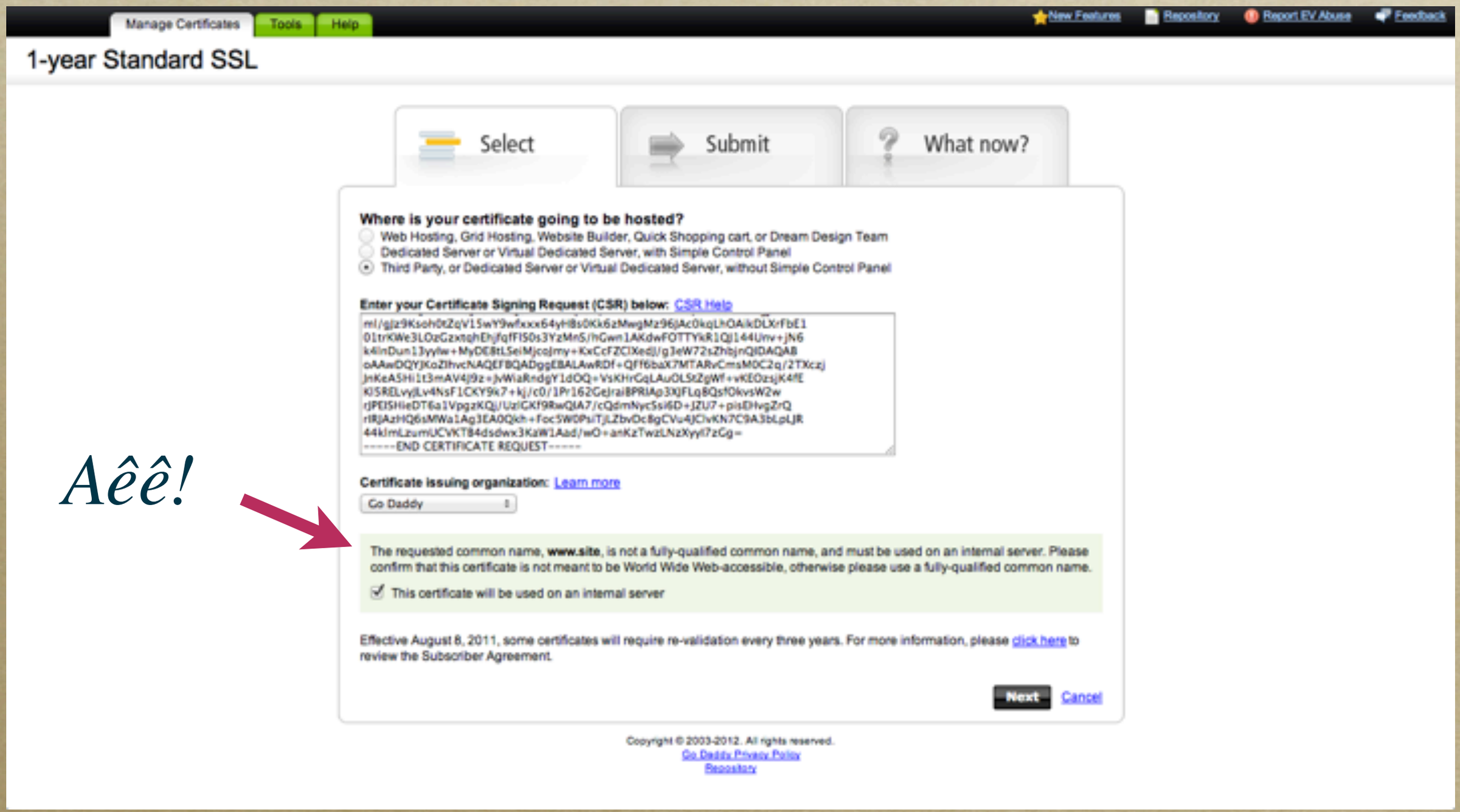
Nomes DNS Internos

- *Imaginados para aplicações restritas à rede interna de uma organização.*
  - *Bastante usados Microsoft Exchange, Active Directory.*
- *www.corp, www.contabil, mail.test*
- *Não terminam em um TLD*
  - *não podem ser usados na Internet*
  - *não há para onde mandar e-mail de validação*

Certificate request: anatomia

```
Certificate Request:
  Data:
   Version: 0 (0x0)
    Subject: C=US, ST=VA, L=Dulles,
    O=Dulles Steel and Forge Supplies,
    OU=IT - Internal WWW Site.,
    CN=www.site/emailAddress=warren@kumari.net
      Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
        RSA Public Key: (2048 bit)
        Modulus (2048 bit):
          00:da:ef:bd:d0:ee:db:...
....
```

Certificado de Uso Interno ?



Aêê!

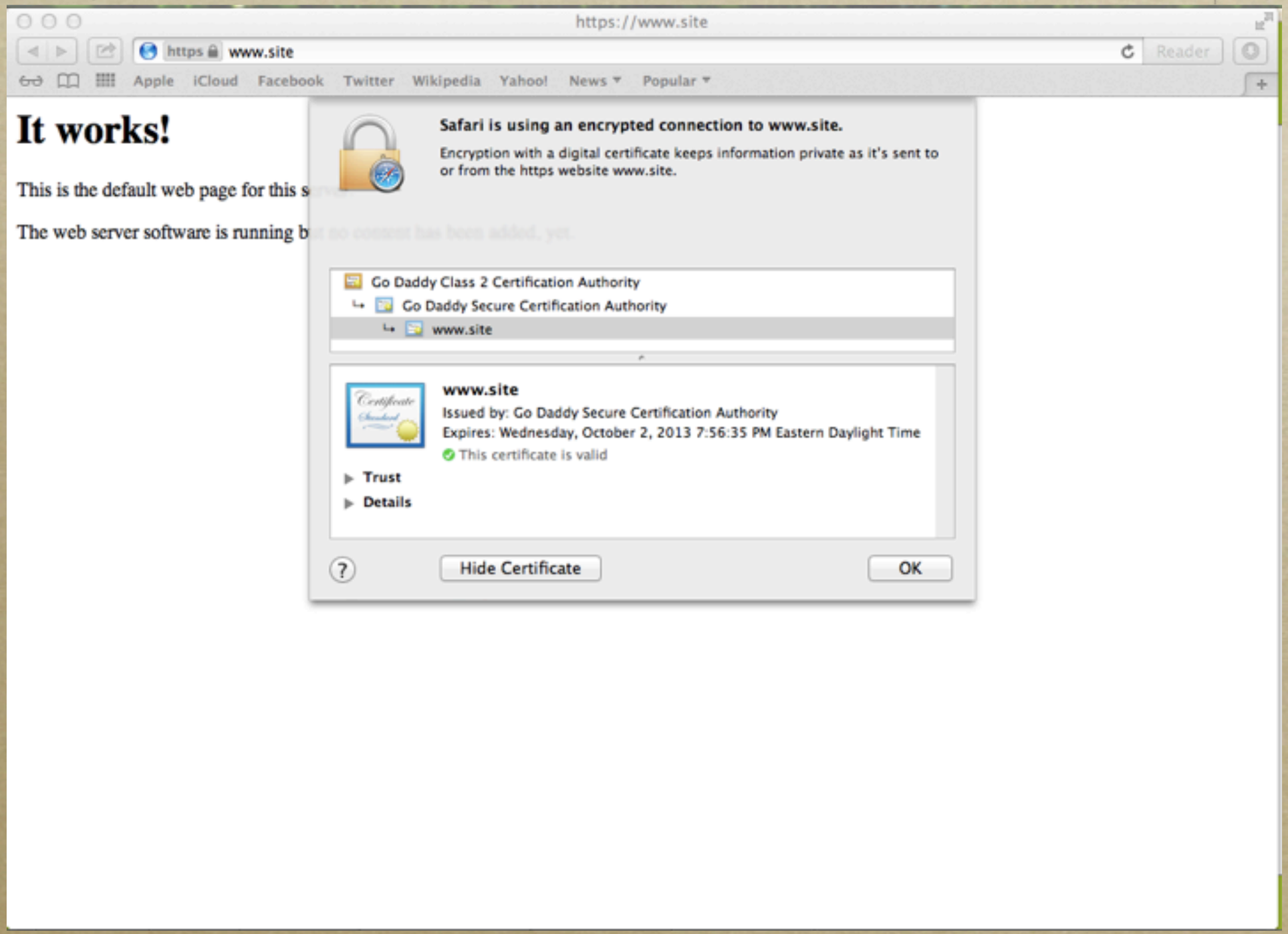
Certificado Emitido

```
Data:
  Version: 3 (0x2)
  Serial Number:
    27:e7:22:63:59:11:b0
  Signature Algorithm: sha1WithRSAEncryption
   Issuer: C=US, ST=Arizona, L=Scottsdale,
    O=GoDaddy.com, Inc., OU=http://
certificates.godaddy.com/repository, CN=Go Daddy Secure
Certification Authority/serialNumber=07969287
    Validity
      Not Before: Oct  2 23:56:35 2012 GMT
      Not After : Oct  2 23:56:35 2013 GMT
  Subject: O=www.site, OU=Domain Control Validated,
           CN=www.site
  X509v3 Subject Alternative Name:
                  DNS:www.site, DNS:site
```

Testes

- *Configurada uma falsa raiz*
- *Delegado .site para o ambiente de teste*
- *Configurado um servidor web, com o certificado emitido*

Doh!


https://www.site
https
www.site
Reader
Apple
iCloud
Facebook
Twitter
Wikipedia
Yahoo!
News
Popular
It works!
This is the default web page for this s
The web server software is running b
Safari is using an encrypted connection to www.site.
Encryption with a digital certificate keeps information private as it's sent to or from the https website www.site.
Go Daddy Class 2 Certification Authority
Go Daddy Secure Certification Authority
www.site
www.site
Issued by: Go Daddy Secure Certification Authority
Expires: Wednesday, October 2, 2013 7:56:35 PM Eastern Daylight Time
This certificate is valid
Trust
Details
Hide Certificate
OK

E daí?

1. *Consiga um certificado para algo que termine num TLD para o qual há candidatura(s).*
2. *Espere o TLD ser delegado.*
3. *Fique à espreita num evento, LAN House, Cyber Café, hotel, ou faça sequestro de DNS, ou corrupção de cache, ou arquivo hosts...*

Investigação

- *SSAC formou um grupo de trabalho*
- *Avaliada ocorrência de certificados não-FQDN*
  - *Usando dados do SSL Observatory da EFF*
  - *1,053 Nomes DNS internos encontrados em certificados, abrangendo 63 possíveis novos TLDs*
    - ***Limite mínimo**, não total, válido quando foi feita a pesquisa*

CA/B Forum

- *Grupo que junta maiores CAs e fabricantes de browsers decidiu apoiar mitigação do problema.*
- *Já tinha começado a invalidar certificados internos(“Baseline Requirements 1.0”), mas decidiu acelerar o processo de alguns anos para 30 dias após assinatura de contrato de novos gTLDs*

Resolvido ? Não...

- *Nem toda CA está no CA/B Forum*
  - *Não estão obrigadas a seguir estes acordos*
    - *Mesmo assim são em geral confiáveis e seguem regras ou do CA/B Forum ou da Mozilla Foundation (que agora também inclui este ponto)*
- *Revogação não é efetiva**
  - *Bloqueio das CRL / OSCP*

* : *http://www.imperialviolet.org/2011/03/18/revocation.html*

Poderia ter sido evitado ?

- *RFC 2606 já reservou .test, .example, .invalid e .localhost em 1999*
- *ICANN em 2012 excluiu também outros TLDs:*

AFRINIC IANA-SERVERS NRO ALAC ICANN RFC-EDITOR APNIC IESG RIPE ARIN IETF ROOT-SERVERS ASO INTERNIC RSSAC CCNSO INVALID SSAC EXAMPLE* IRTF TEST* GAC ISTF TLD GNSO LACNIC WHOIS GTLD-SERVERS LOCAL WWW IAB LOCALHOST IANA NIC

- *draft-ceshire-dnsext-multicastdns-02 de 2003 citava .intranet, .internal, .private, .corp e .home (RFC 6762 cita também .lan)*
- *SAC 045: TLDs inválidos em queries a root servers*

Perguntas?