Authentication. Security. Trust.

GlobalSign®

A tutorial on how you can host **multiple SSL Certificates on a single IP address** without losing any backward compatibility

Paul van Brouwershaven
Business Development Director EMEA, GlobalSign
@vanbroup on Twitter

Paul van Brouwershaven

Netherlands

Business Development Director

- Business Development Director for GlobalSign
- Previously CTO of a European hosting company
- Over 10 years of **experience in the hosting industry**
- Expert in digital certificate solutions
- Dedicated to increasing awareness of the requirements for online security
- Thinking out of the box, detecting problems and providing solutions

GlobalSign®
GMO INTERNET GROUP

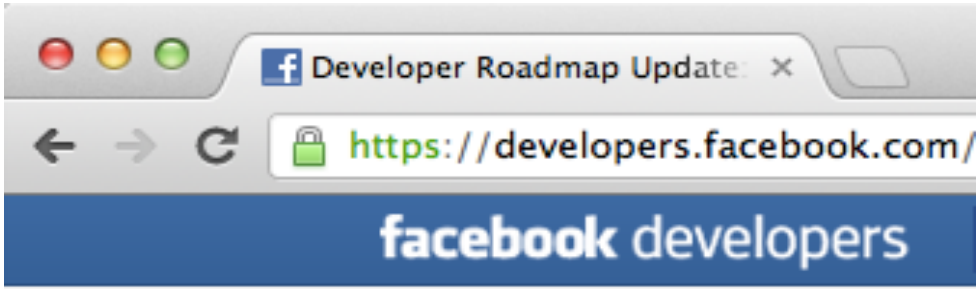
Multiple SSL Certificates on a single IP address

More demands and requirements for SSL

Article 17 of Directive 95/46/EC of the European Parliament
Security of processing

Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

PCI Security Standards Council™

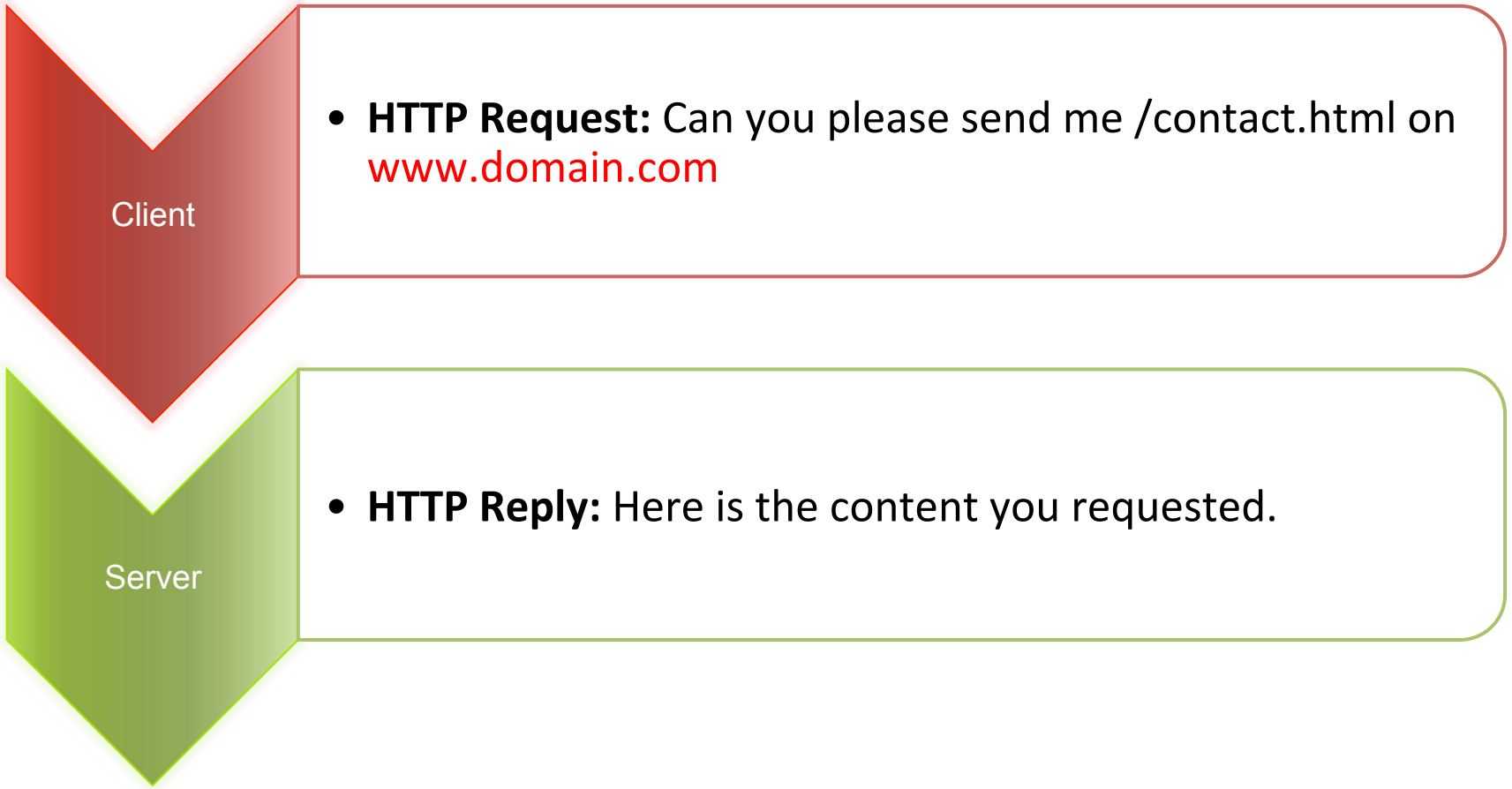


NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

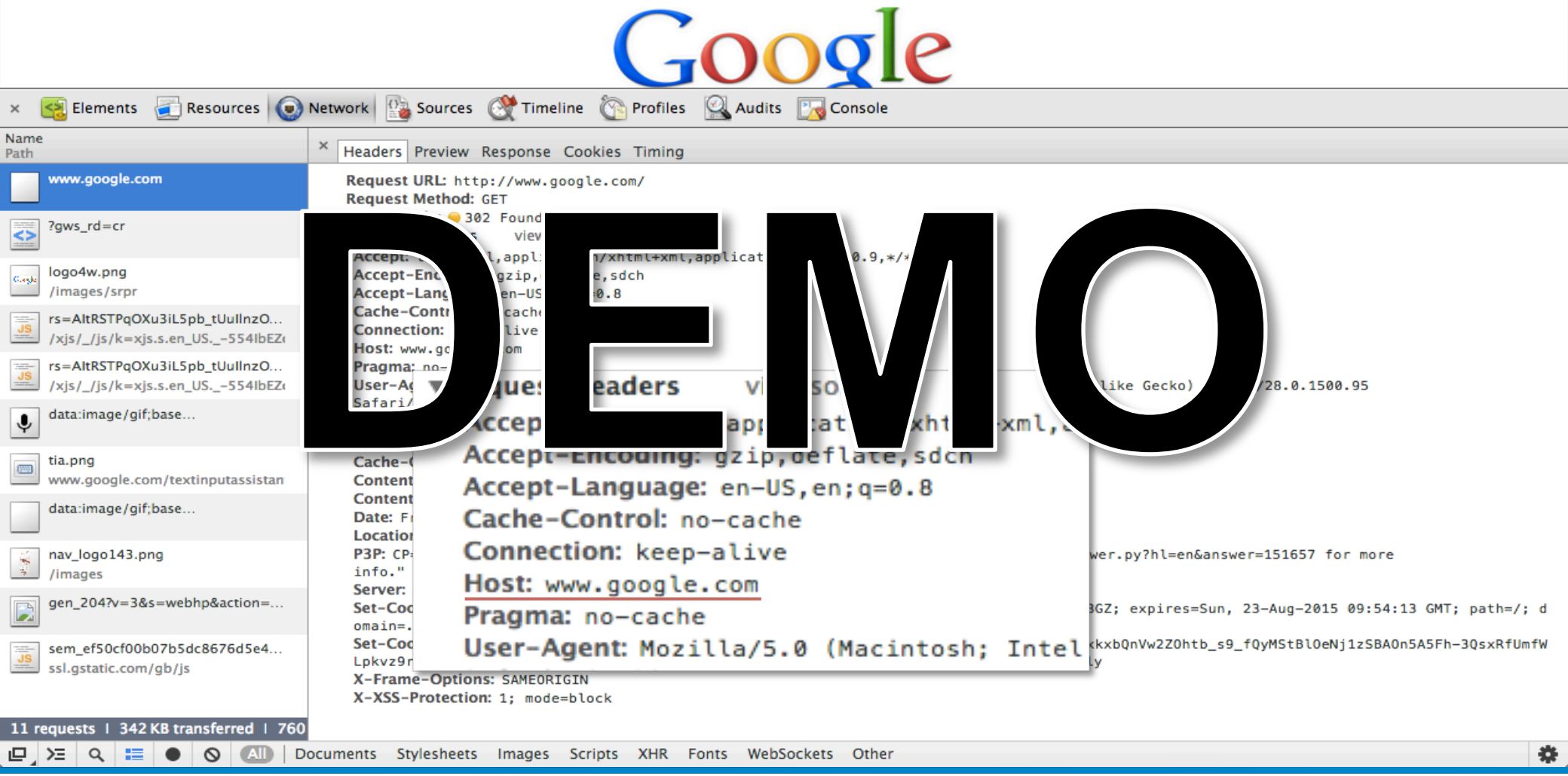
Each SSL Certificate needs its own IP

Why do I need a dedicated IP address?

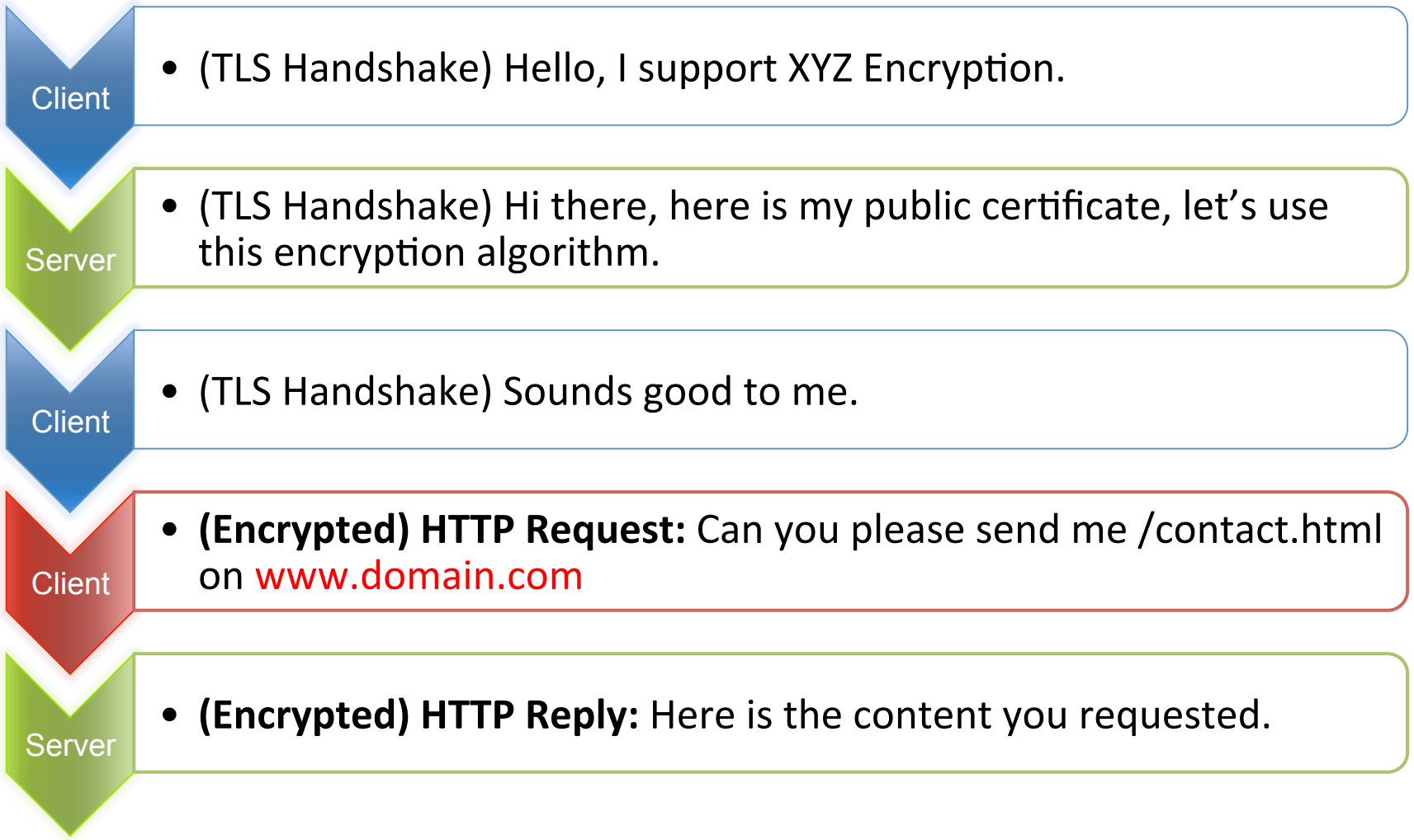
Request on a non-secure connection



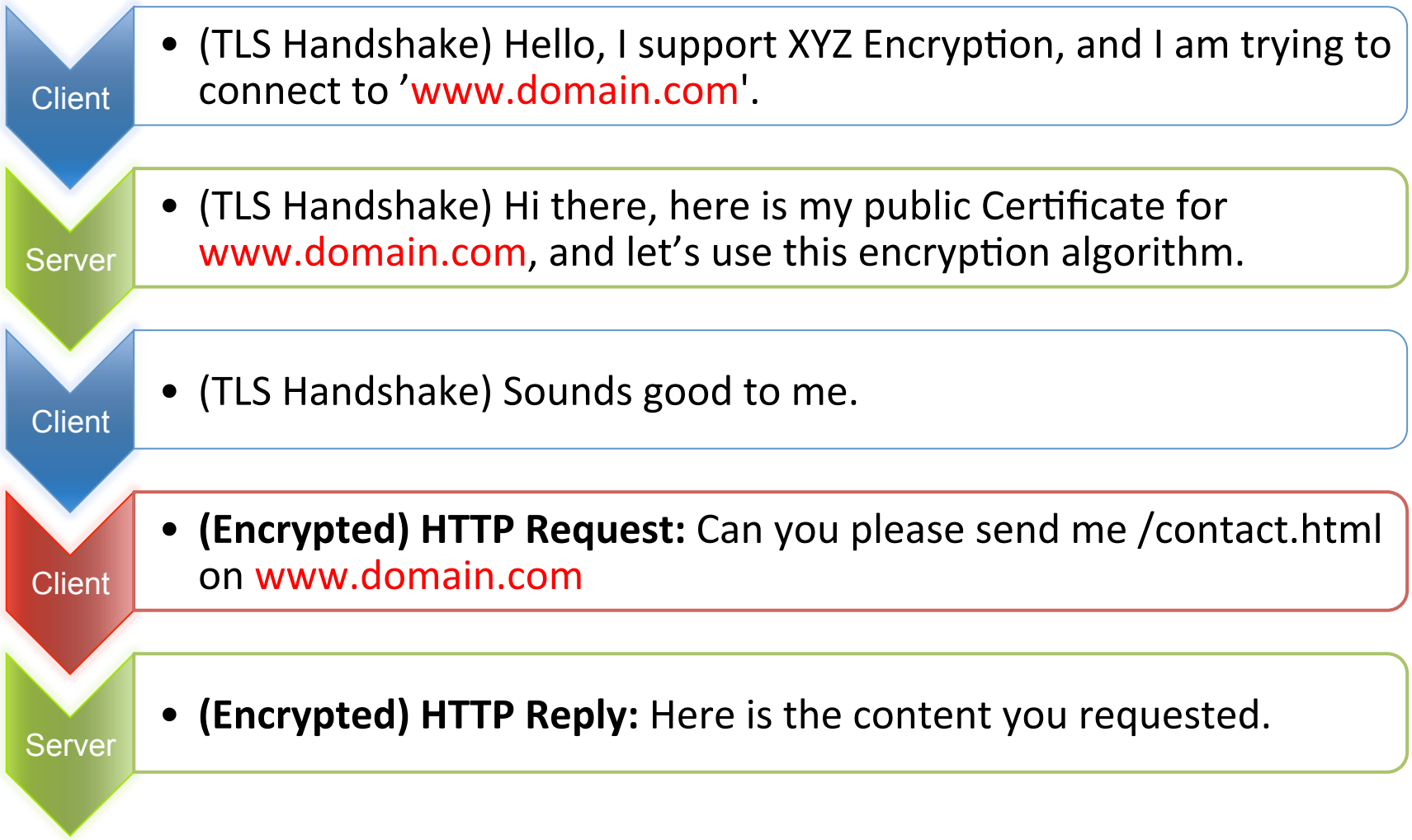
Host: www.domain.com



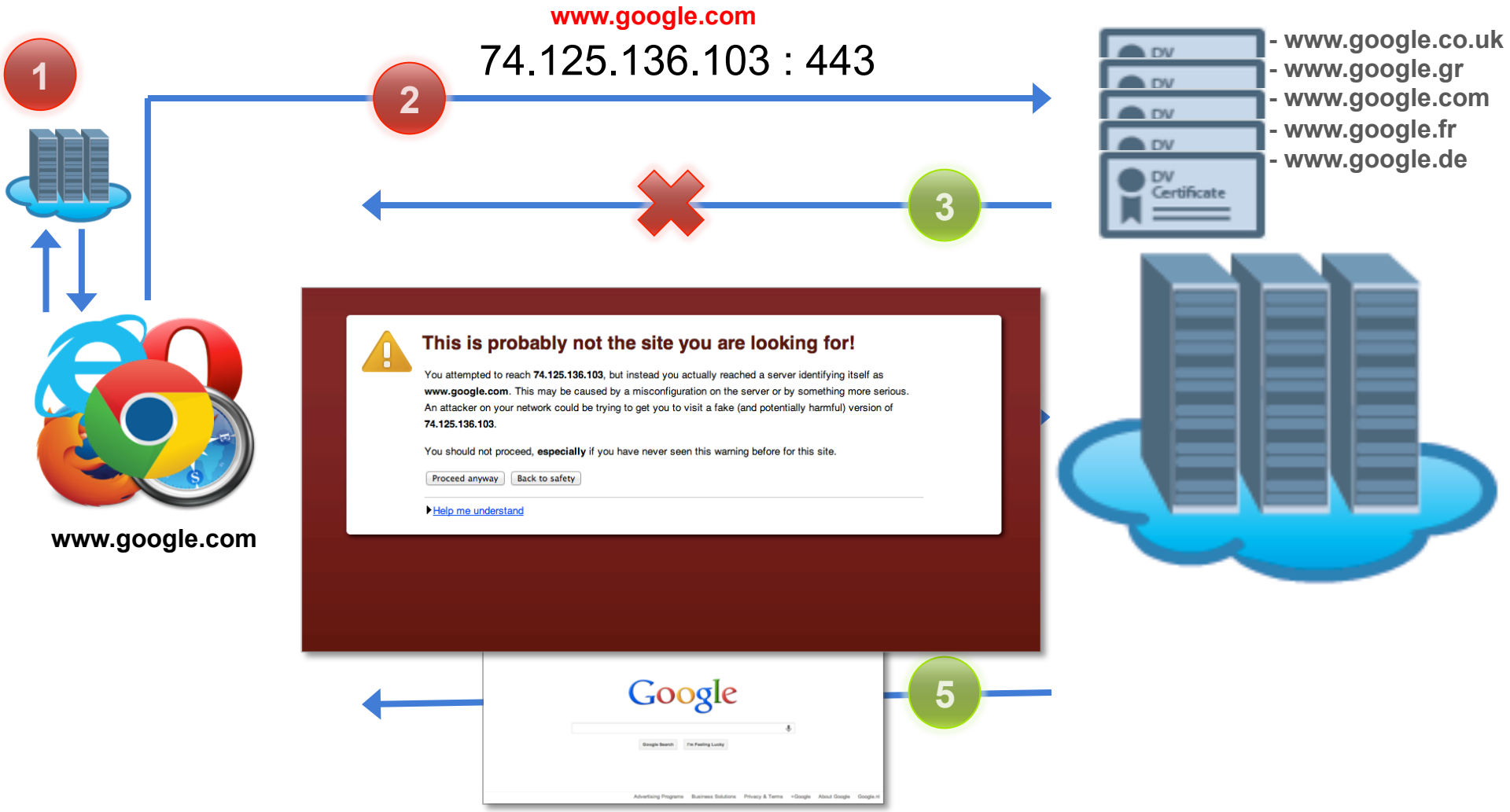
Request on a secure connection



Server Name Indication (SNI)



Request on a secure connection



Testing SNI with OpenSSL

DEMO

The SSL/TLS handshake

```
2013-02-22 13:55:26.884043000 192.168.1.242     www.globalsign.com  TLSv1.1  Client Hello
2013-02-22 13:55:26.964894000 www.globalsign.com 192.168.1.242      TLSv1.1  Server Hello
2013-02-22 13:55:26.969102000 www.globalsign.com 192.168.1.242      TLSv1.1  Certificate, Server Key Exchange,
2013-02-22 13:55:26.982744000 192.168.1.242     www.globalsign.com  TLSv1.1  Client Key Exchange, Change Cipher
2013-02-22 13:55:27.070372000 www.globalsign.com 192.168.1.242      TLSv1.1  New Session Ticket, Change Cipher
```

```
▽ TLSv1.1 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 179
  ▽ Handshake Protocol: Client Hello
      Handshake Type: Client Hello (1)
      Length: 175
      Version: TLS 1.2 (0x0302)
    ▷ Random
      Session ID Length: 0
      Cipher Suites Length: 72
    ▷ Cipher Suites (36 suites)
      Compression Methods Length: 1
    ▷ Compression Methods (1 method)
      Extensions Length: 62
    ▽ Extension: server_name
        Type: server_name (0x0000)
        Length: 23
      ▽ Server Name Indication extension
          Server Name list length: 21
          Server Name Type: host_name (0)
          Server Name length: 18
          Server Name: www.globalsign.com
    ▷ Extension: renegotiation_info
    ▷ Extension: elliptic_curves
```

DEMO

```
▽ Extension: server_name
    Type: server_name (0x0000)
    Length: 23
  ▽ Server Name Indication extension
      Server Name list length: 21
      Server Name Type: host_name (0)
      Server Name length: 18
      Server Name: www.globalsign.com
```

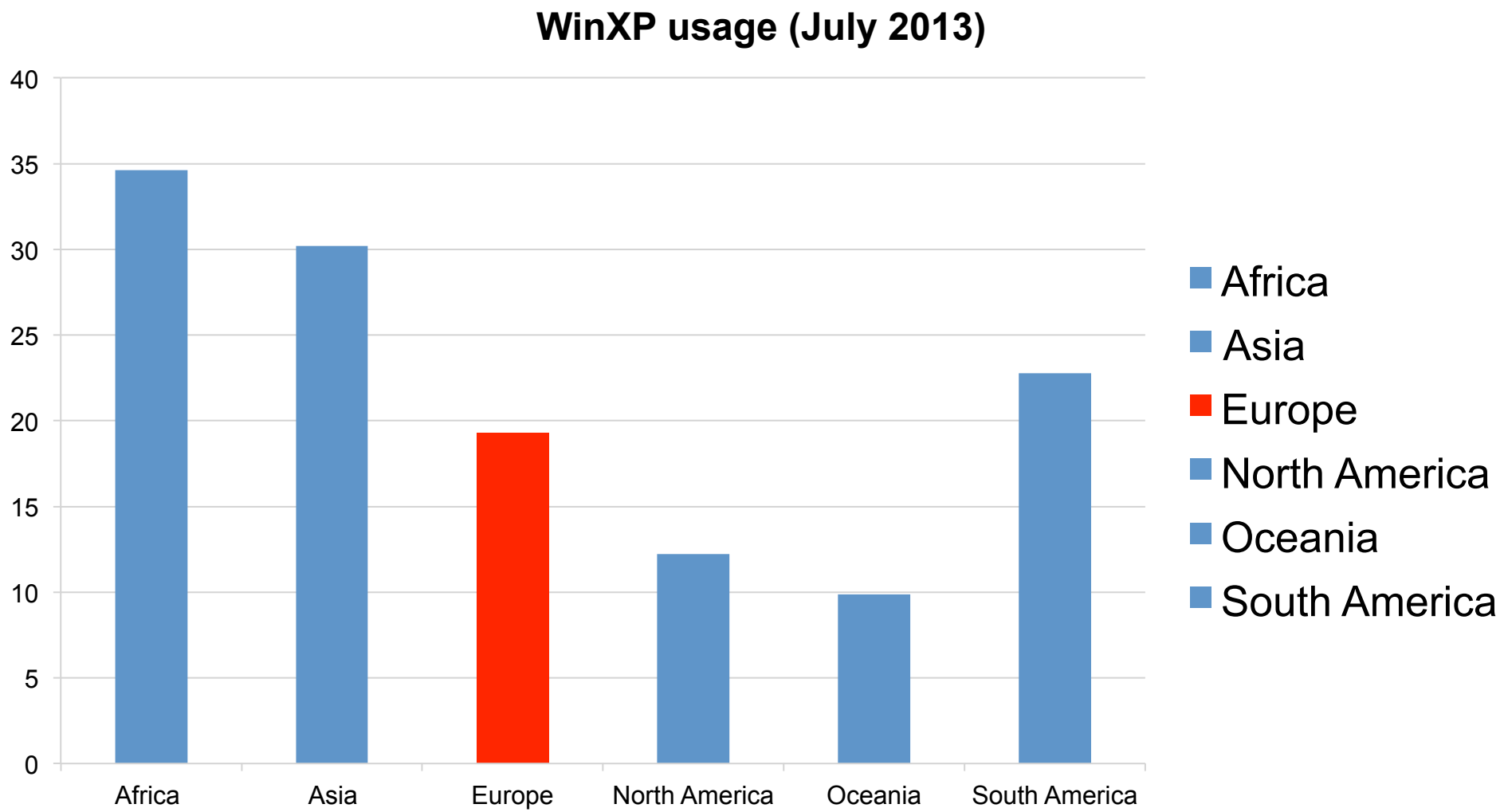
Applications with no SNI Support

- All versions of Internet Explorer on Windows XP
- Android 2.x [Gingerbread] default browser (other browsers like Opera do support SNI on Android)
- BlackBerry Browser
- Windows Mobile up to 6.5

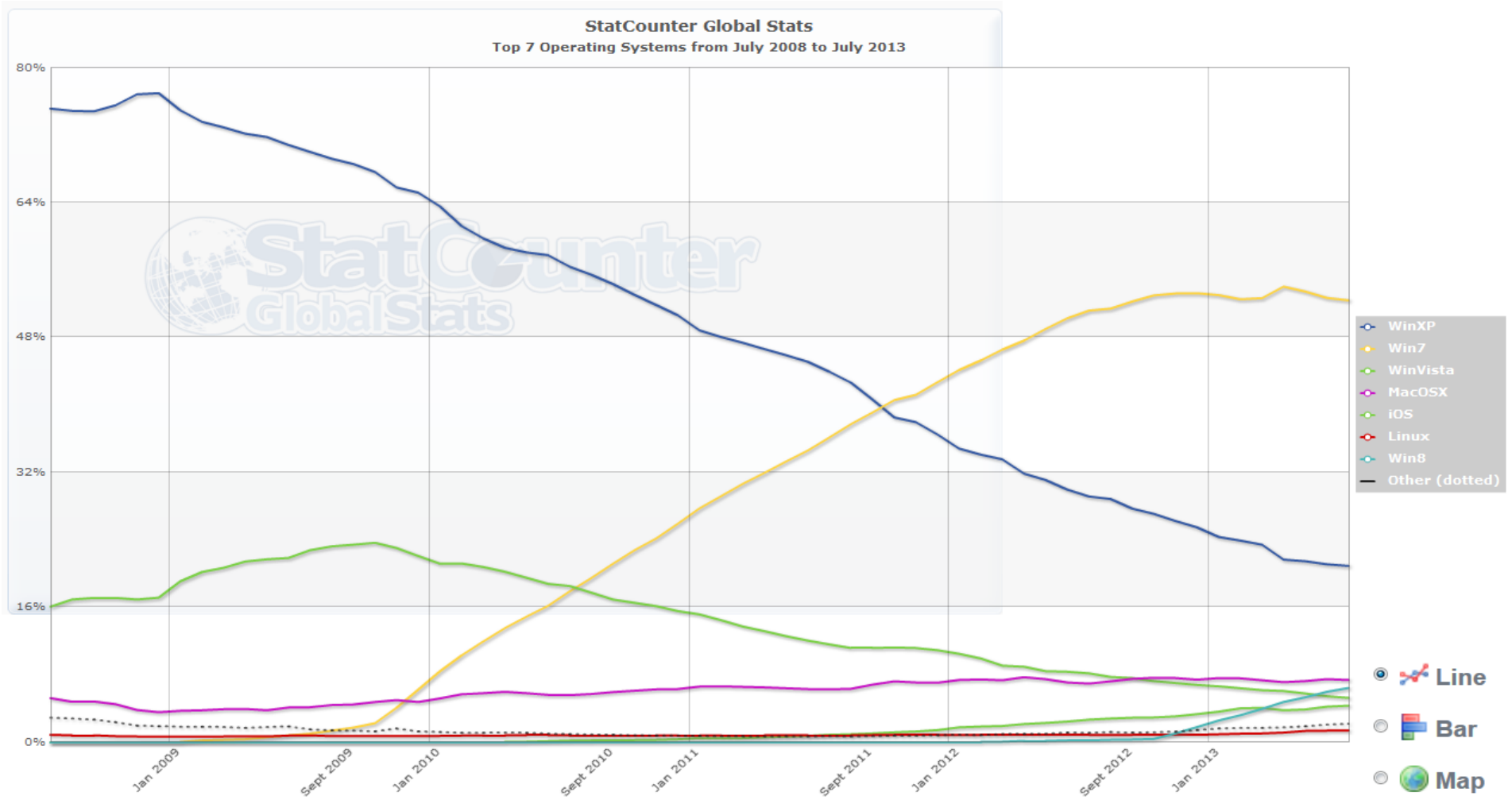
Windows XP with SNI

DEMO

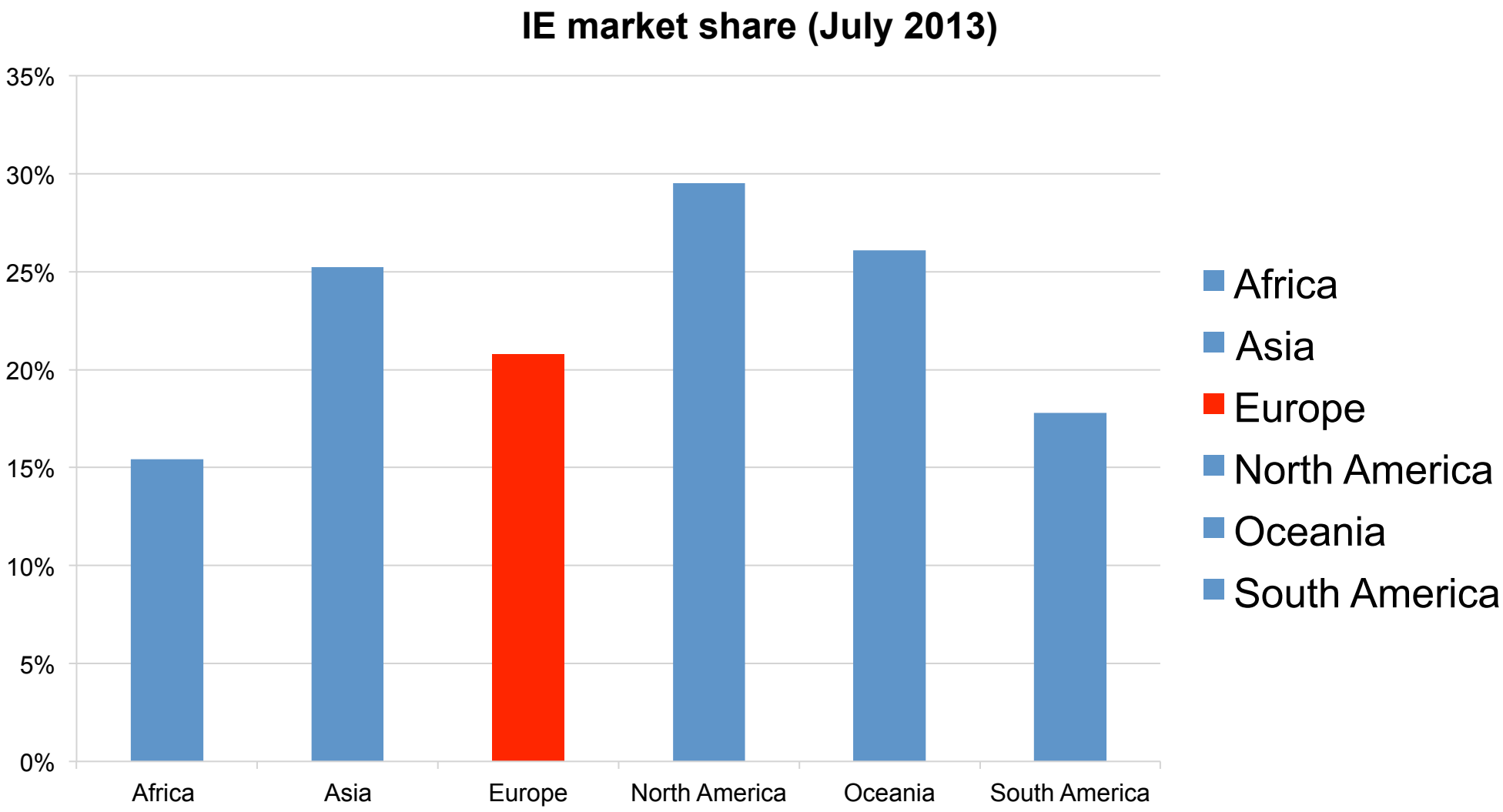
Operating System Usage - Win XP – per continent



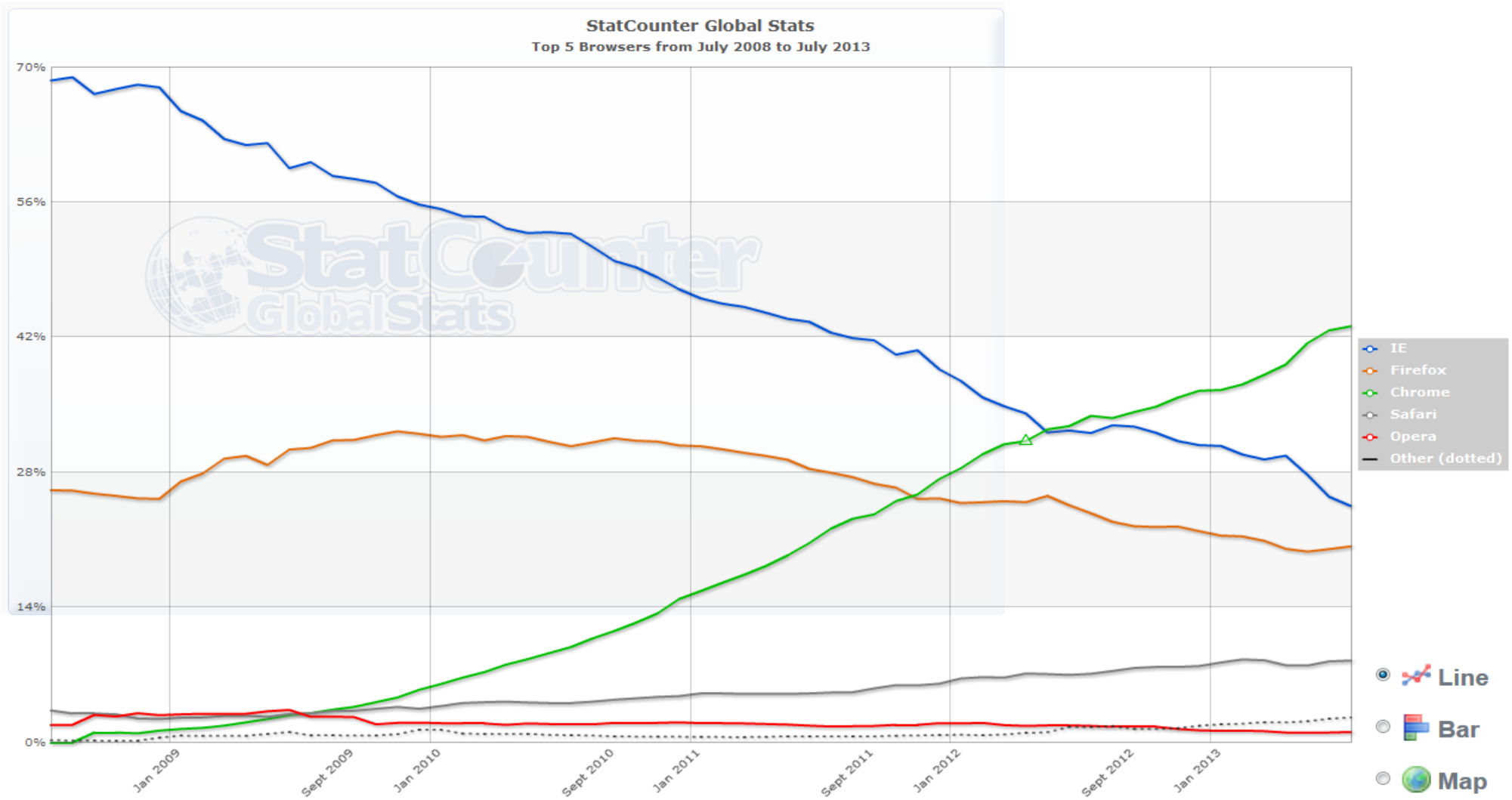
Worldwide Operating System Usage - Win XP: 21%



Internet Explorer market share – Per continent



Worldwide Internet Explorer market share – 25%



Or 8% of your world wide visitors?

25% of 21% = 5.3%

Internet Explorer Windows XP

+ mobile traffic

=

8% of World Wide internet users do not support Server Name Indication (SNI)

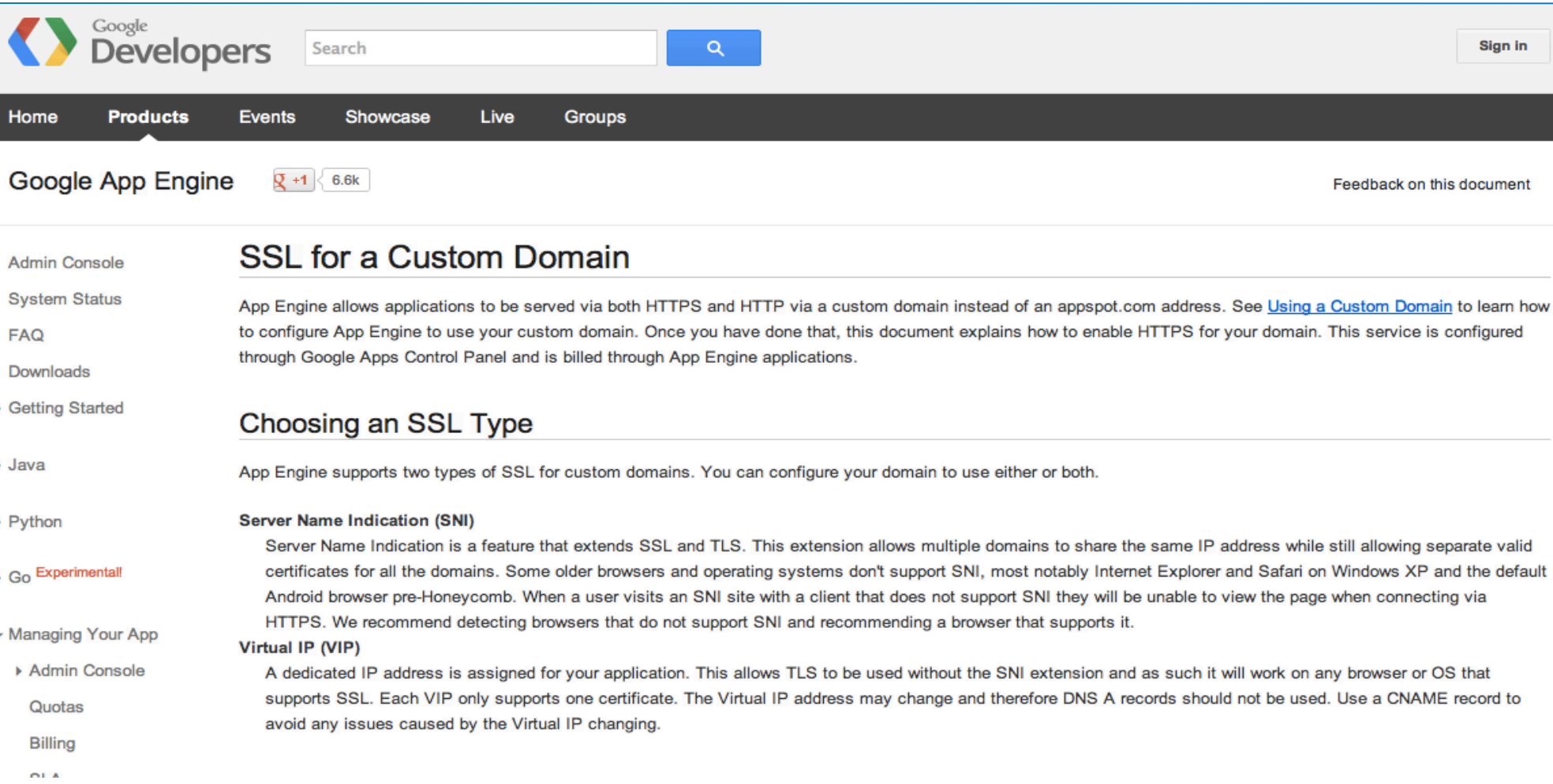
Should I use/offer SNI for SSL sites?

- There is no problem when you need to secure a website or portal that is used by a closed community or business that has no Windows XP users.

- Provide SNI support for free with an SSL Certificate
  - Users can decide to provide an unsecure connection and a warning to visitors with an outdated system.

- Calculate an additional fee for users that want to have full compatibility and thus a dedicated IP number

Should I use/offer SNI for SSL sites?



Google Developers

Search

Sign in

Home | Products | Events | Showcase | Live | Groups

Google App Engine +1 6.6k

Feedback on this document

- Admin Console
- System Status
- FAQ
- Downloads
- Getting Started
- Java
- Python
- Go Experimental!
- Managing Your App
  - Admin Console
  - Quotas
  - Billing

SSL for a Custom Domain

App Engine allows applications to be served via both HTTPS and HTTP via a custom domain instead of an appspot.com address. See Using a Custom Domain to learn how to configure App Engine to use your custom domain. Once you have done that, this document explains how to enable HTTPS for your domain. This service is configured through Google Apps Control Panel and is billed through App Engine applications.

Choosing an SSL Type

App Engine supports two types of SSL for custom domains. You can configure your domain to use either or both.

Server Name Indication (SNI)

Server Name Indication is a feature that extends SSL and TLS. This extension allows multiple domains to share the same IP address while still allowing separate valid certificates for all the domains. Some older browsers and operating systems don't support SNI, most notably Internet Explorer and Safari on Windows XP and the default Android browser pre-Honeycomb. When a user visits an SNI site with a client that does not support SNI they will be unable to view the page when connecting via HTTPS. We recommend detecting browsers that do not support SNI and recommending a browser that supports it.

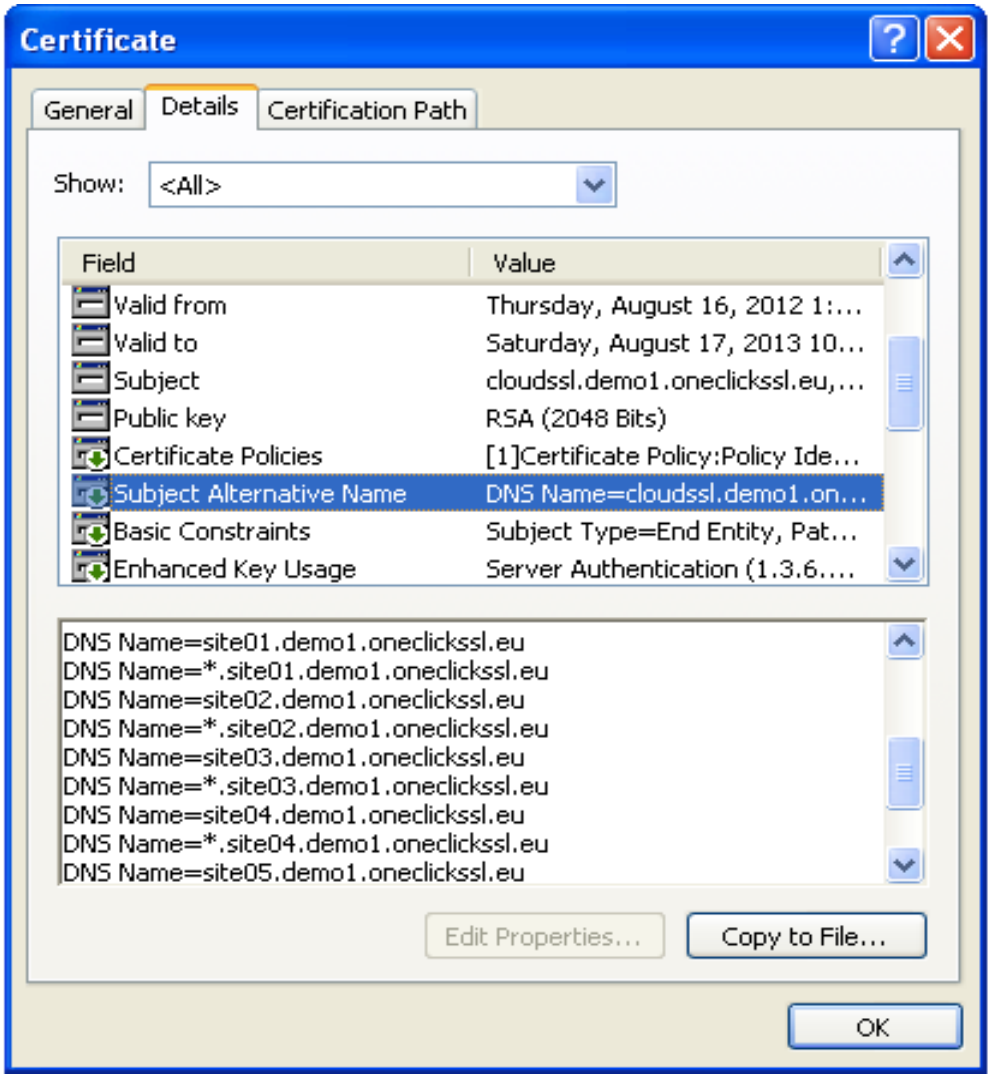
Virtual IP (VIP)

A dedicated IP address is assigned for your application. This allows TLS to be used without the SNI extension and as such it will work on any browser or OS that supports SSL. Each VIP only supports one certificate. The Virtual IP address may change and therefore DNS A records should not be used. Use a CNAME record to avoid any issues caused by the Virtual IP changing.

What are the alternative solutions?

A multi-domain SSL Certificate

- One SSL Certificate for multiple domain names from different organisations.
- The certificate contains the hosting company's details.
- Domain control is verified for each domain.



Multi-domain certificates

DEMO

Control of the Private Key

- A multi-domain certificate usually runs on shared hosting server or reversed proxy DN
- Domain control is validated for each SAN
- SSL Certificate accessible by server or network administrator with root permissions
- Information of the company that is responsible for the private key is listed in the certificate contents.

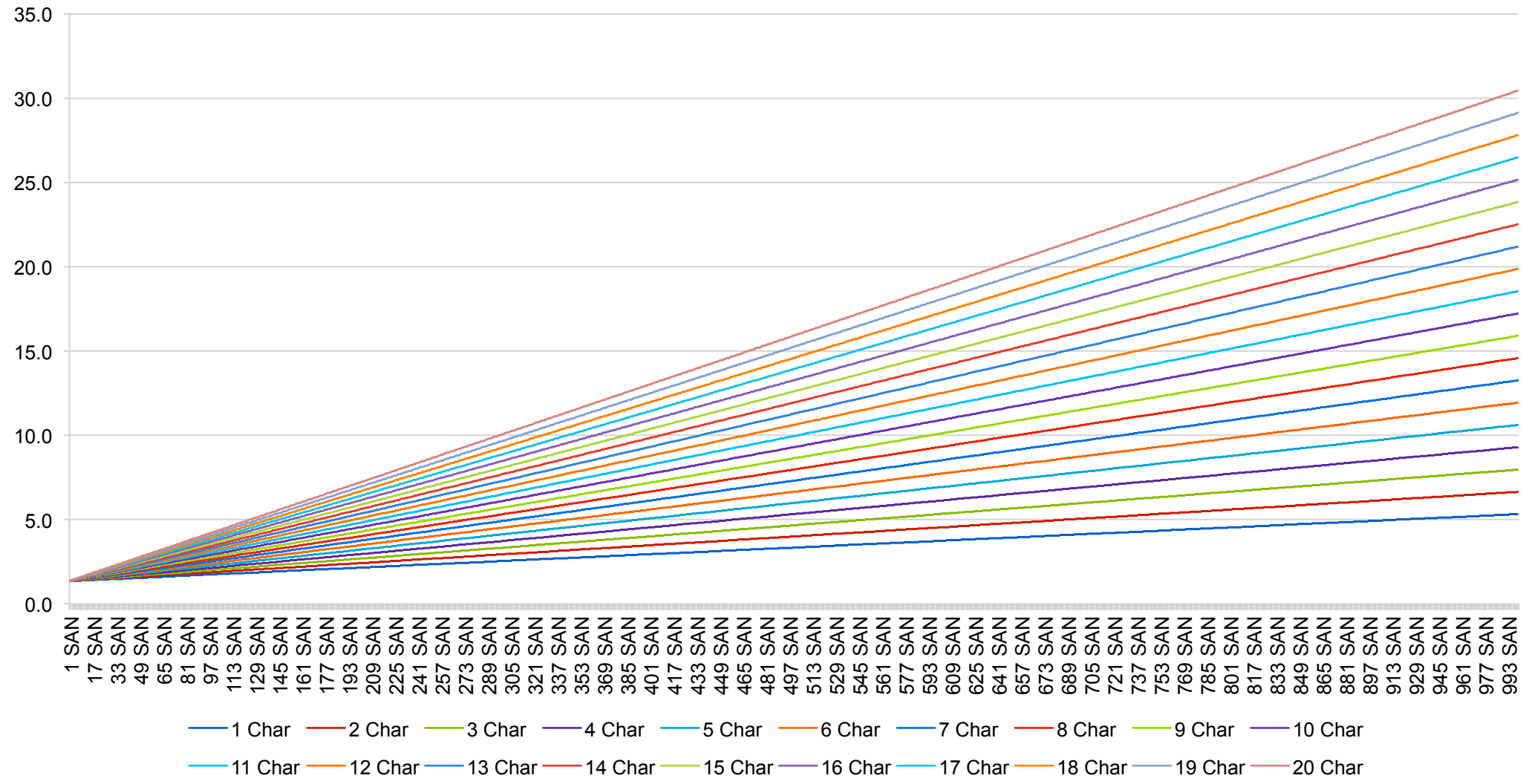
Certificate Size

	1 Char	2 Char	3 Char	4 Char	5 Char	6 Char	7 Char	8 Char	9 Char	10 Char	11 Char	12 Char	13 Char	14 Char	15 Char	16 Char	17 Char	18 Char	19 Char	20 Char
1 SAN	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4
2 SAN	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4
3 SAN	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4
4 SAN	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.5	1.5	1.5	1.5
5 SAN	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.5	1.5	1.5	1.5	1.5	1.5	1.5
640 SAN	3.9	4.7	5.6	6.4	7.3	8.1	9.0	9.8	10.7	11.5	12.4	13.2	14.1	14.9	15.8	16.6	17.4	18.3	19.1	20.0
641 SAN	3.9	4.8	5.6	6.4	7.3	8.1	9.0	9.8	10.7	11.5	12.4	13.2	14.1	14.9	15.8	16.6	17.5	18.3	19.2	20.0
709 SAN	4.2	5.1	6.1	7.0	7.9	8.9	9.8	10.7	11.7	12.6	13.5	14.5	15.4	16.4	17.3	18.2	19.2	20.1	21.1	22.0
710 SAN	4.2	5.1	6.1	7.0	7.9	8.9	9.8	10.8	11.7	12.6	13.6	14.5	15.4	16.4	17.3	18.3	19.2	20.1	21.1	22.0
711 SAN	4.2	5.1	6.1	7.0	7.9	8.9	9.8	10.8	11.7	12.6	13.6	14.5	15.5	16.4	17.3	18.3	19.2	20.2	21.1	22.0
748 SAN	4.3	5.3	6.3	7.3	8.3	9.3	10.3	11.3	12.2	13.2	14.2	15.2	16.2	17.2	18.2	19.2	20.2	21.1	22.1	23.1
749 SAN	4.3	5.3	6.3	7.3	8.3	9.3	10.3	11.3	12.3	13.2	14.2	15.2	16.2	17.2	18.2	19.2	20.2	21.2	22.2	23.2
750 SAN	4.3	5.3	6.3	7.3	8.3	9.3	10.3	11.3	12.3	13.3	14.3	15.2	16.2	17.2	18.2	19.2	20.2	21.2	22.2	23.2
998 SAN	5.3	6.6	8.0	9.3	10.6	11.9	13.2	14.6	15.9	17.2	18.5	19.8	21.2	22.5	23.8	25.1	26.4	27.8	29.1	30.4
999 SAN	5.3	6.6	8.0	9.3	10.6	11.9	13.3	14.6	15.9	17.2	18.5	19.9	21.2	22.5	23.8	25.1	26.5	27.8	29.1	30.4
1000 SAN	5.3	6.7	8.0	9.3	10.6	11.9	13.3	14.6	15.9	17.2	18.6	19.9	21.2	22.5	23.8	25.2	26.5	27.8	29.1	30.5

- Test results based on number of SANs and characters
- Note: Average number of characters in a domain – 13/14*

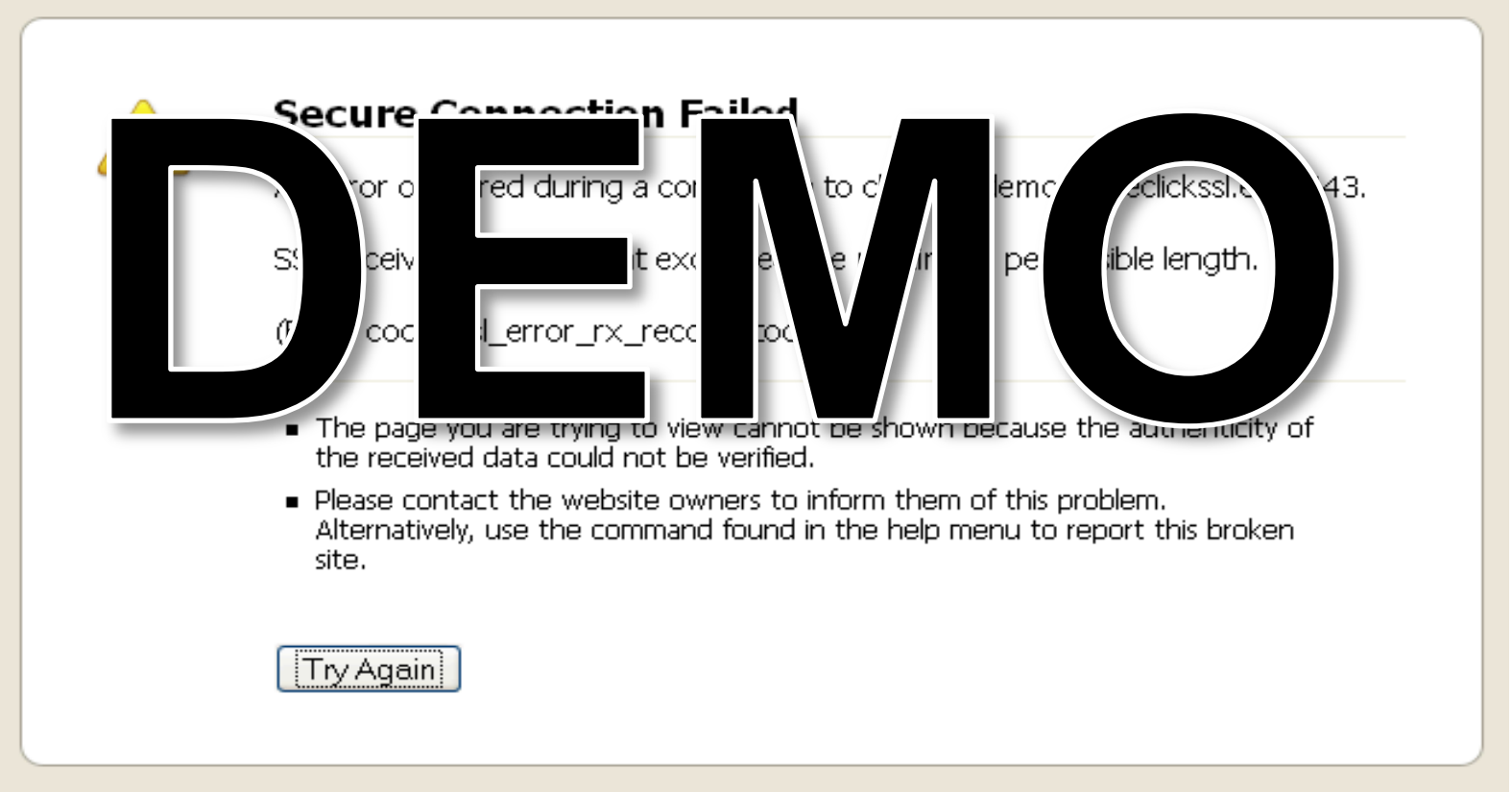
  **Source: Nominet*
- Certificate size limit is browser dependent

Certificate Growth



Maximum Certificate Size

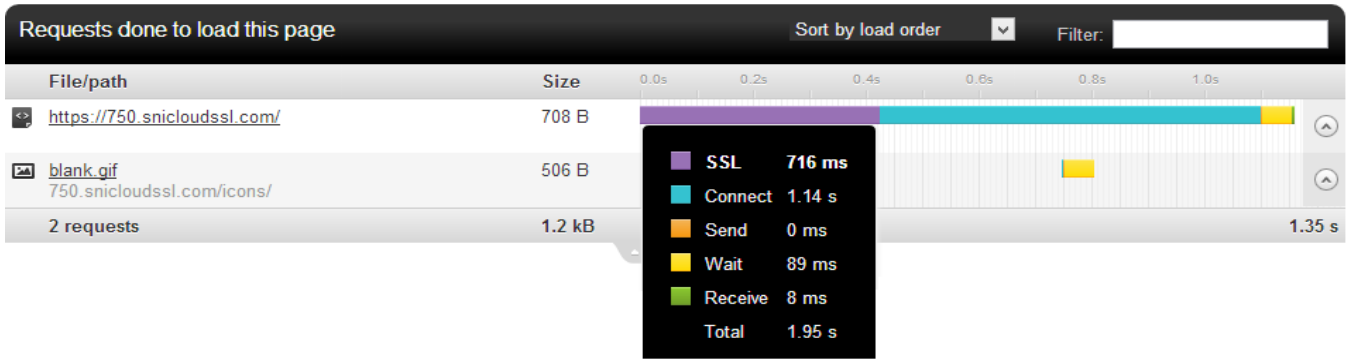
- Google Chrome, Mozilla Firefox & Opera have a limit of 174K.



Maximum Certificate Size

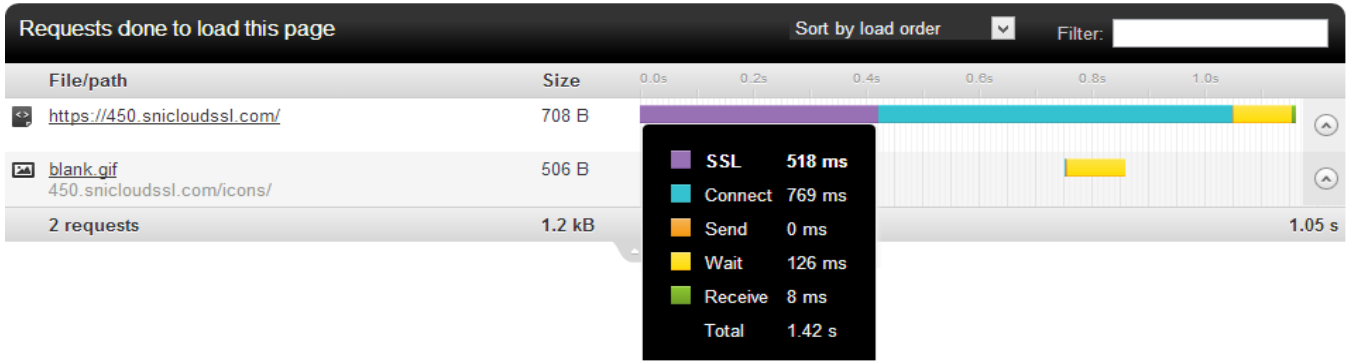
- Internet Explorer on Windows XP SP3 till Windows 7 has a certificate size limit of 44k.
- Windows XP without any service packs is limited to 22k.
- An average OCSP stapling response is about 1k
- Other TLS overhead is about 0.5k

Performance of multi-domain certificates



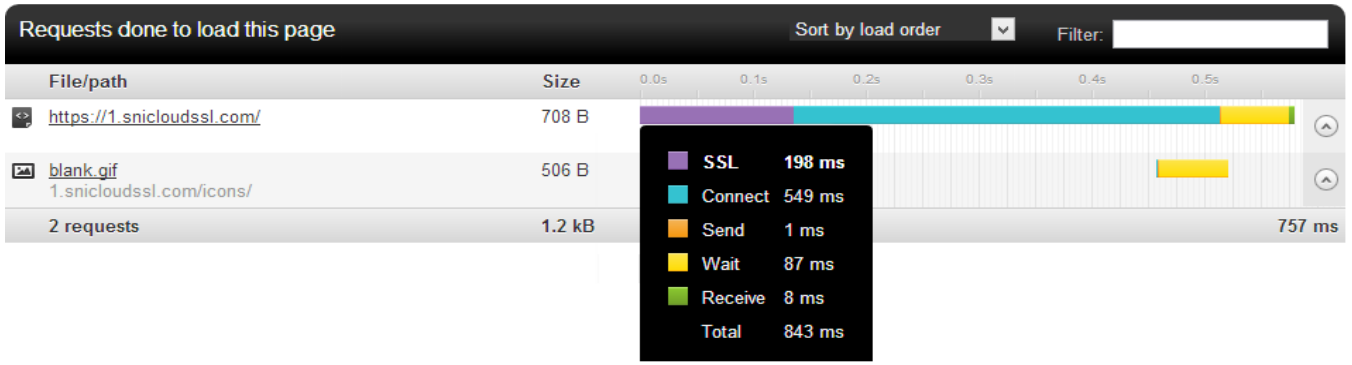
- 750 names:

716 ms



- 450 names:

518 ms



- 1 name:

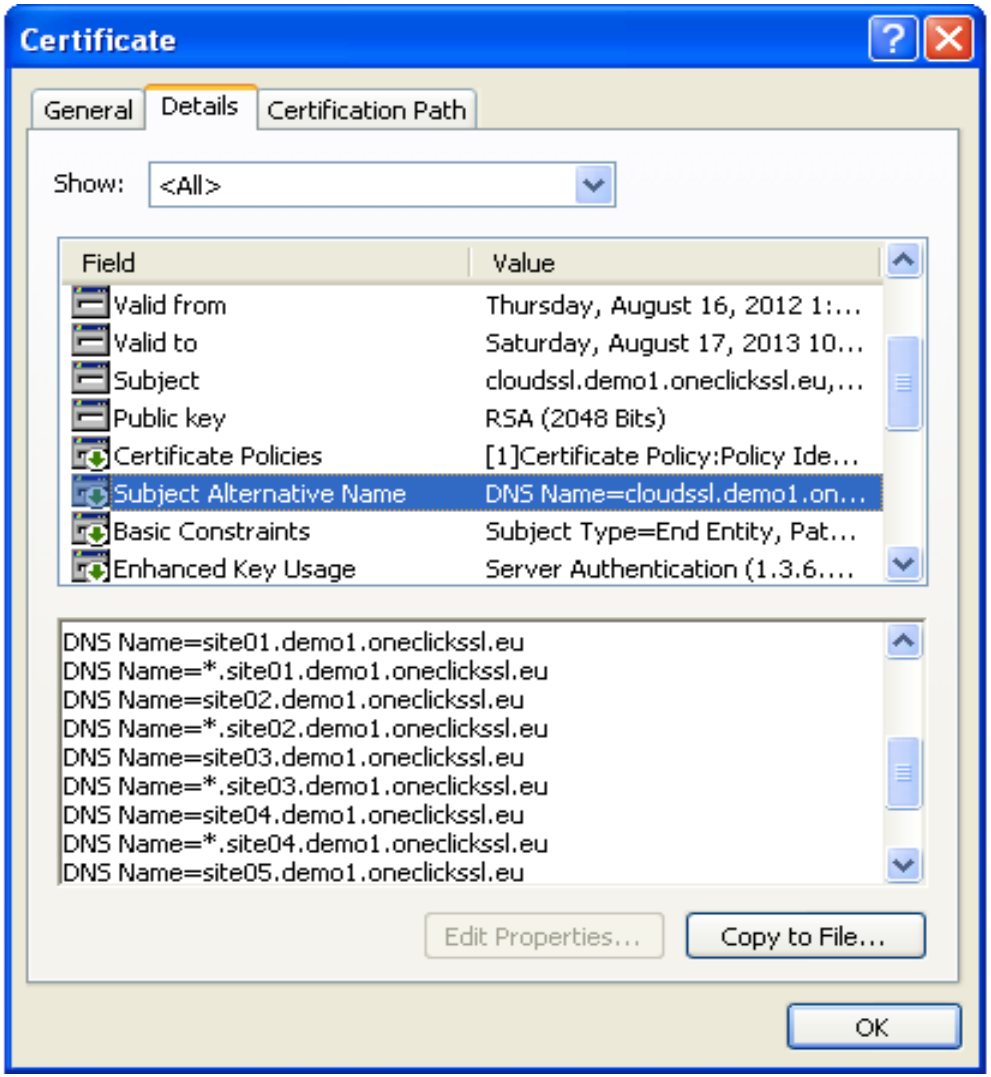
198 ms

Every 100ms delay costs 1% of sales

amazon.com®

The disadvantages of multi-domain certs

- No support for OV, EV
- One certificate shared by many websites
- Many hostnames are visible in the certificate
- Visitor needs to download a bigger certificate (slower)

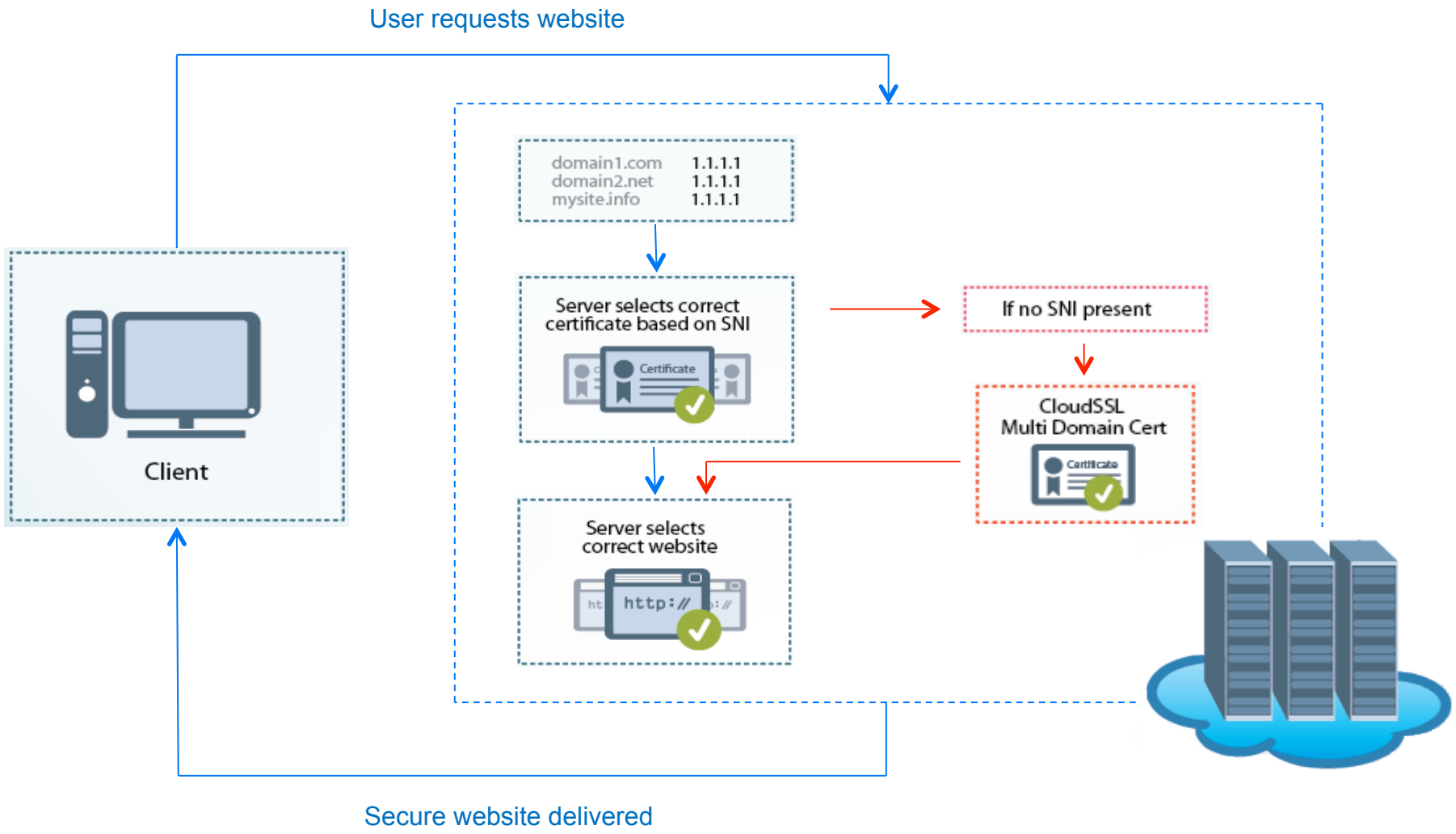


What if we could use the best of both solutions?

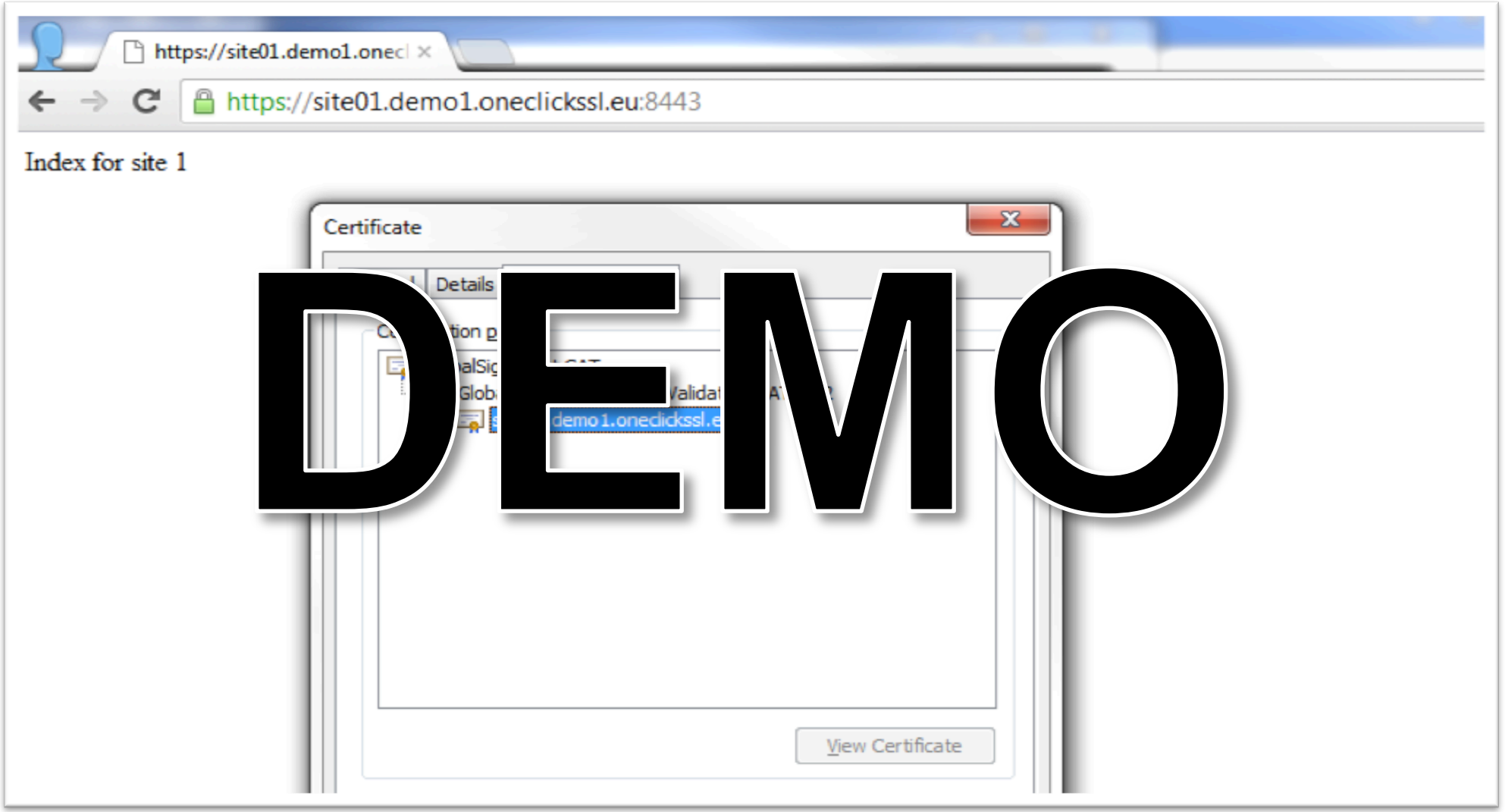
92% SNI

/ 8% CloudSSL

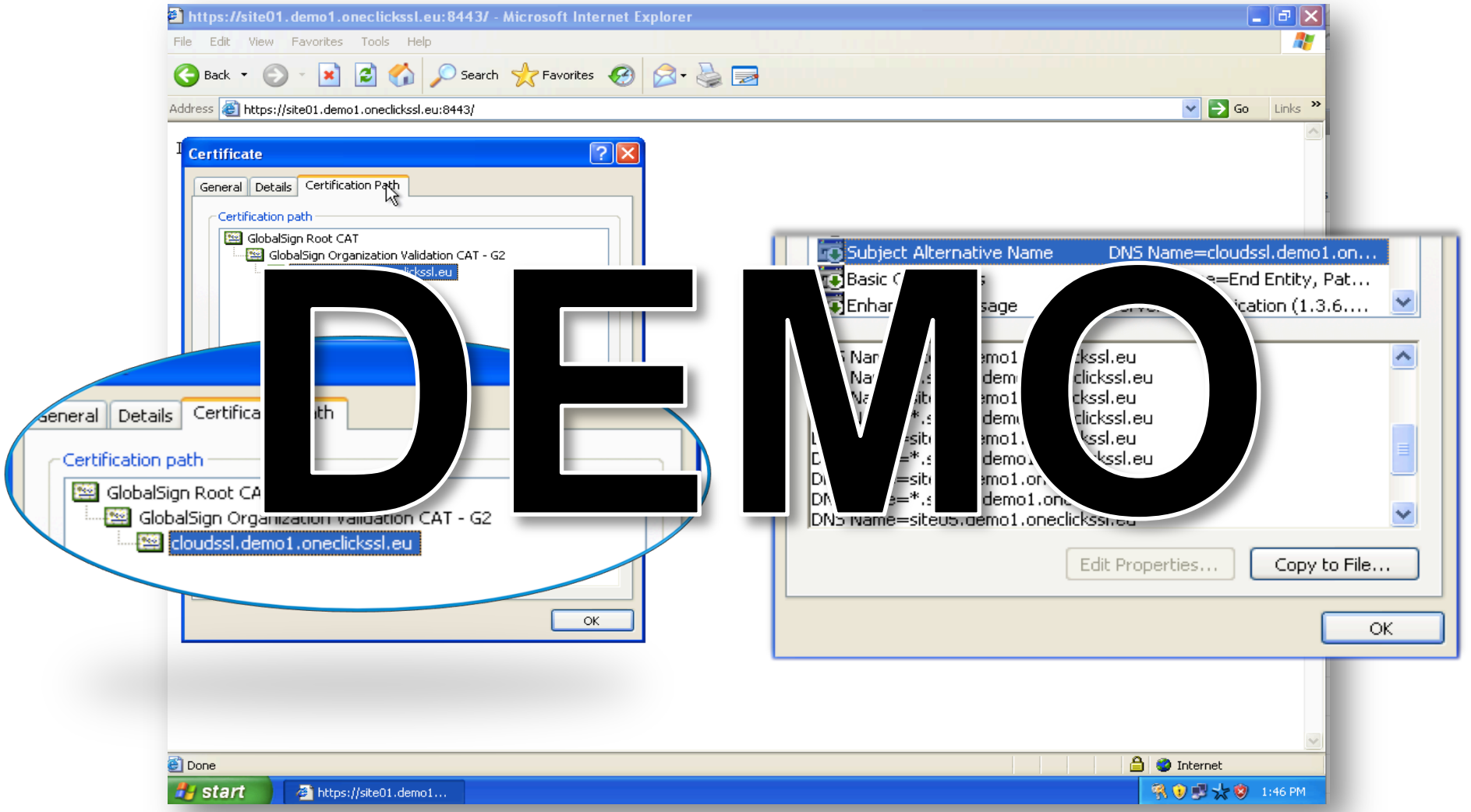
SNI combined with CloudSSL



With SNI support



Windows XP (has no SNI support)



How Google Implemented this

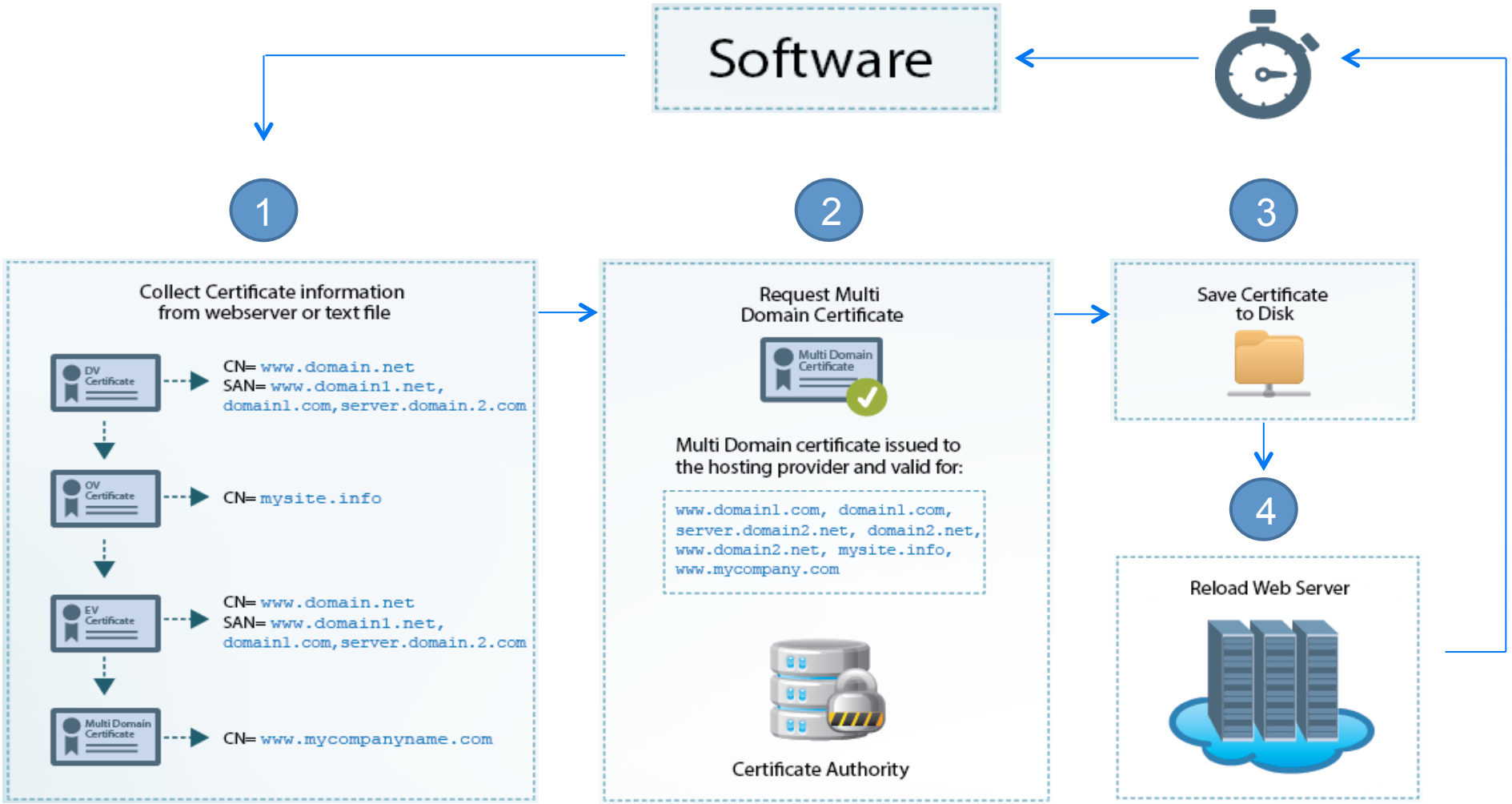
DEMO

Two SSL Certificates for one site!

- No additional costs
- Sites can use all types of certificates (including EV)
- One SSL Certificate installed via the regular way, a second SSL Certificate (one per IP) can be updated automatically.

Environment and Platform independent

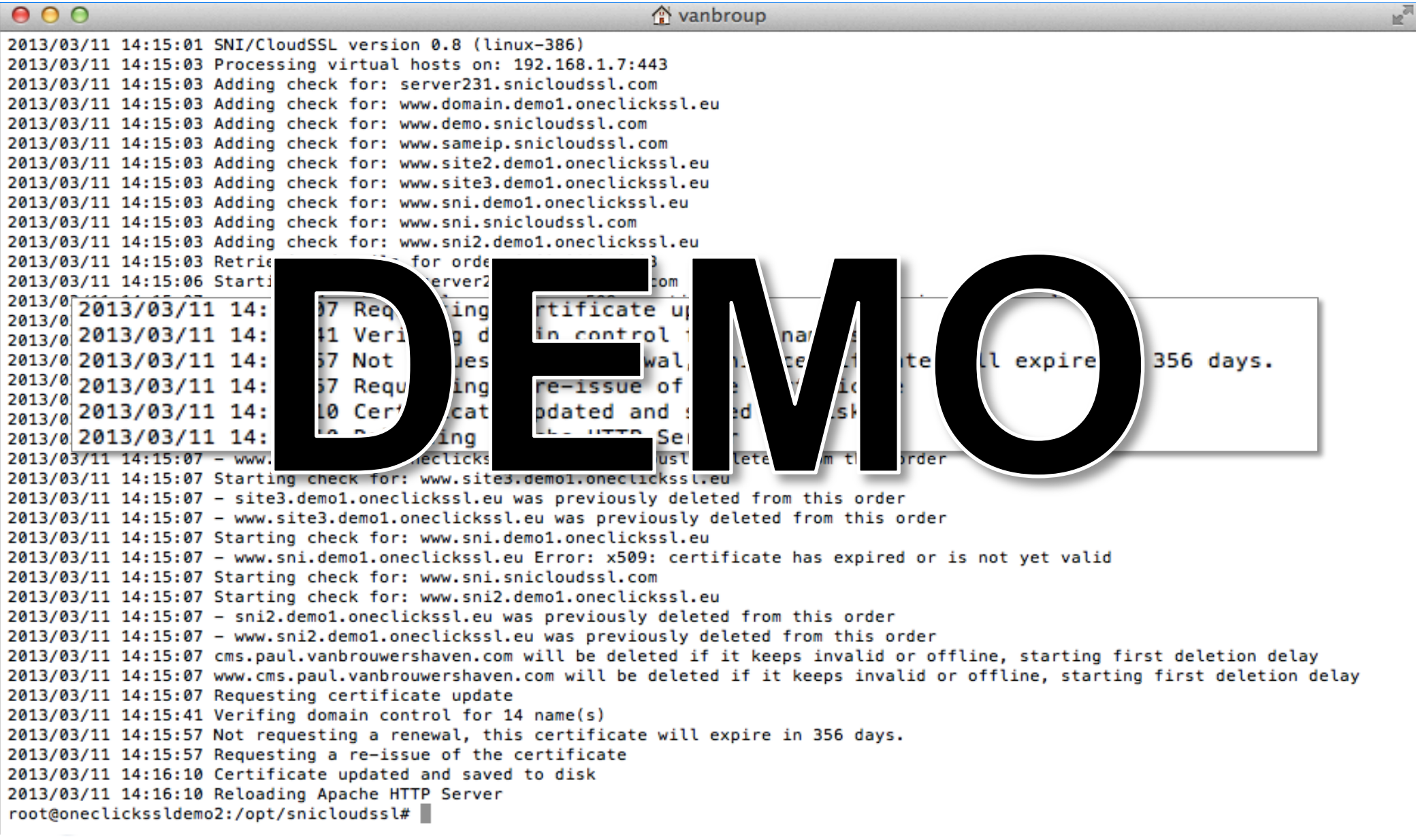
How does it work?



Lets create a few sites in DirectAdmin

DEMO

Completely Automated Process



Automated domain control validation

User Agent Redirect

Apache

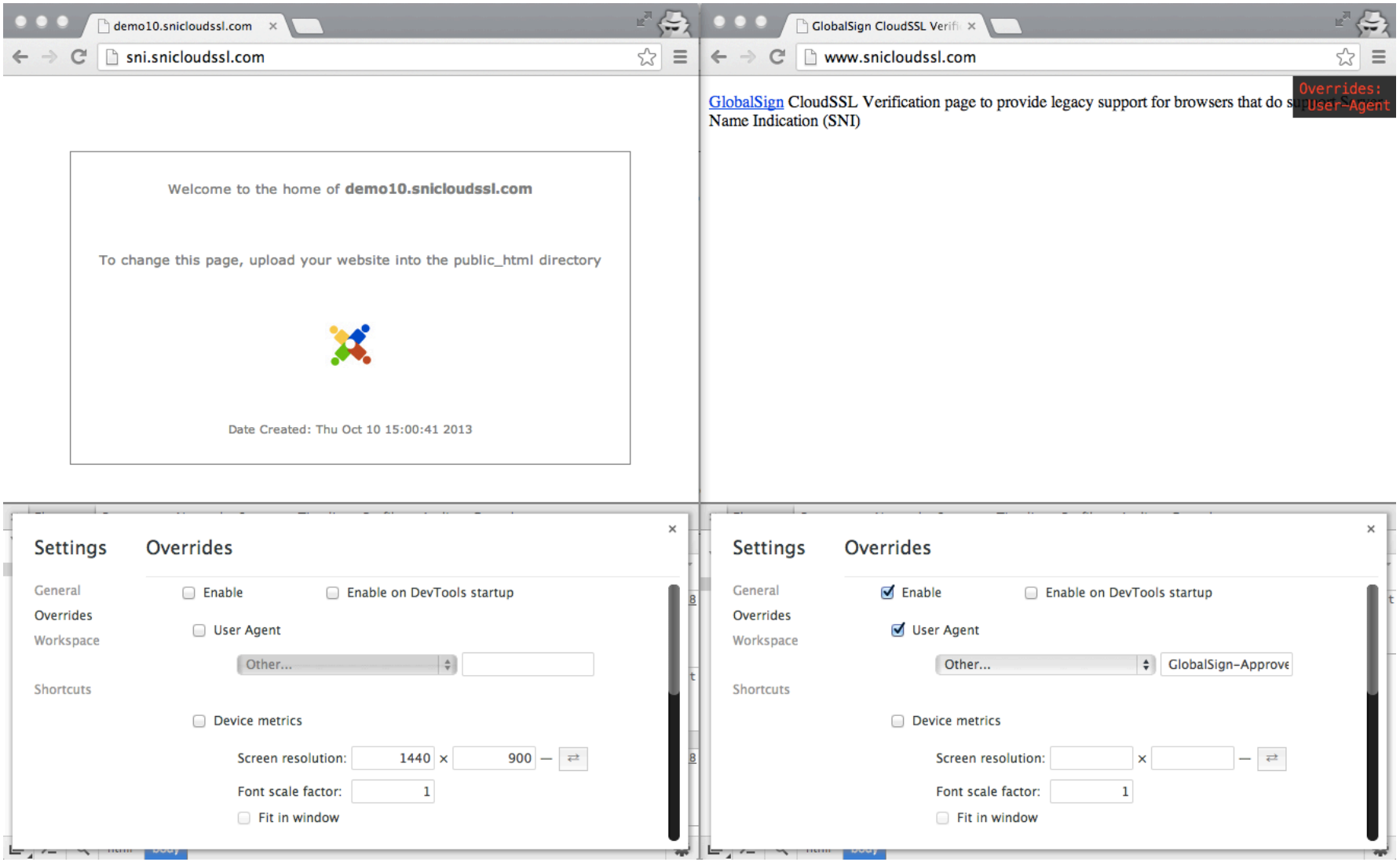
```
RewriteEngine On
RewriteCond  %{HTTP_USER_AGENT}  ^GlobalSign
RewriteRule  ^/$                 /opt/snicloudssl/html/index.html
```

NGINX

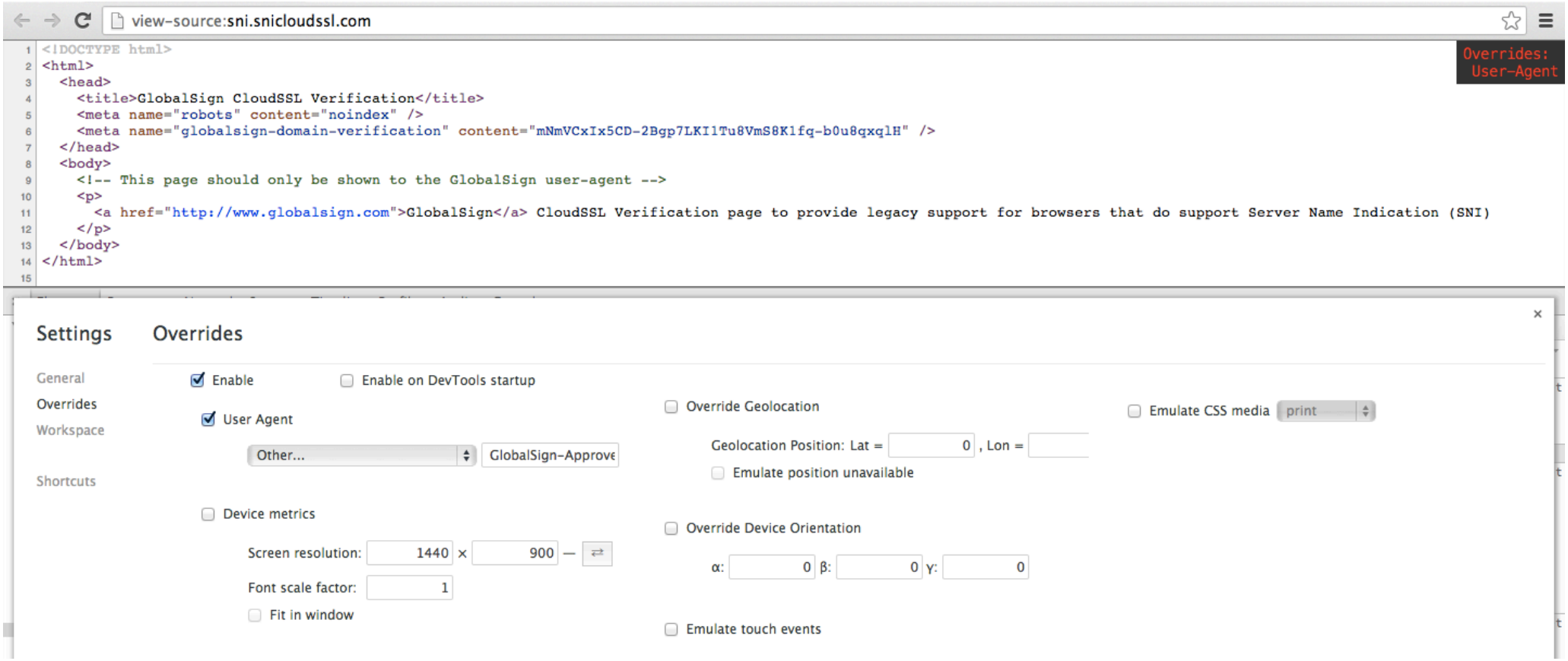
```
if ( $http_user_agent ~* ^GlobalSign.* ) {
    rewrite ^/(.*)$ /gscloudsslvalidaion/index.html last;
}

location /gscloudsslvalidaion {
    alias /opt/snicloudssl/html/;
}
```

Same site, Different content



Using meta-tag authentication



Using meta-tag authentication

▼ **Request Headers** view source

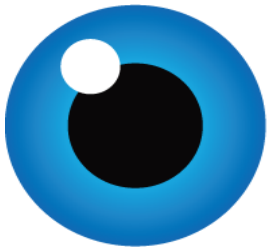
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Encoding: gzip,deflate,sdch
Accept-Language: en-US,en;q=0.8,nl;q=0.6
Cache-Control: no-cache
Connection: keep-alive
Host: sni.snicloudssl.com
Pragma: no-cache
User-Agent: GlobalSign-Approver-URL-Domain-Control-Verification-Agent-www.globalsign.com

Thank you

Paul van Brouwershaven

paul.vanbrouwershaven@globalsign.com

@vanbroup



GlobalSign®