

Authentication. Security. Trust.



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  
@vanbrou on Twitter

# Paul van Brouwershaven



A word cloud featuring various technical and business terms. The most prominent words include: **development**, **security**, **social**, **certificate**, **linux**, **mysql**, **php**, **validation**, **marketing**, **ipsec**, **business**, **windows**, **perl**, **ssl**, **golang**, **creative**, **integrity**, **signing**, **development**, **security**, **social**, **certificate**. Other visible words include: global, sign, data, nessus, kvm, server, s/mime, programming, problem, self-confidence, document, presenting, communications, network, process, software, databases, professional, product, php, validation, ipv, business, dnssec, marketing, quagga, novell, cloud, pki, api, routing, solving, bash, arin, computing, mysql, name, code, scripting, ms-sql, linux, whois, perl, tls, mining, responsibility, thinking, java, bgp, speaker, phyton, pades, new, mariadb, networks, messaging, epp, ospf, international, linkedin, domain, centos, pdf, cisco, openbsd, apple, rip, apache, online, leadership, debian, snort, clustering, learner, dns, google, iptables, architecture, macos, ripe, seo, loyalty, cgi, golang, anycast, solaris, networking, soap.



# 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





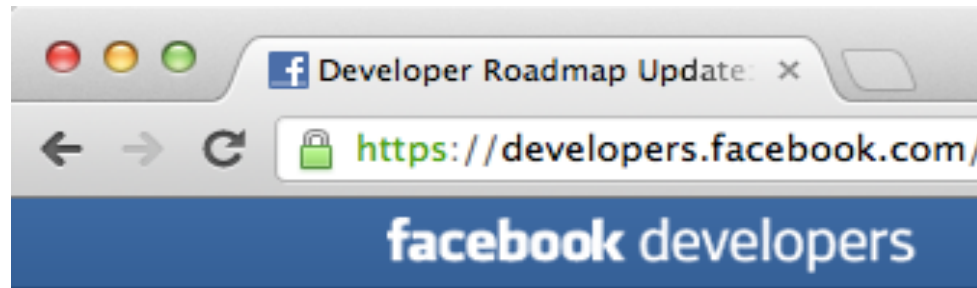
# Multiple SSL Certificates on a single IP address



# 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.





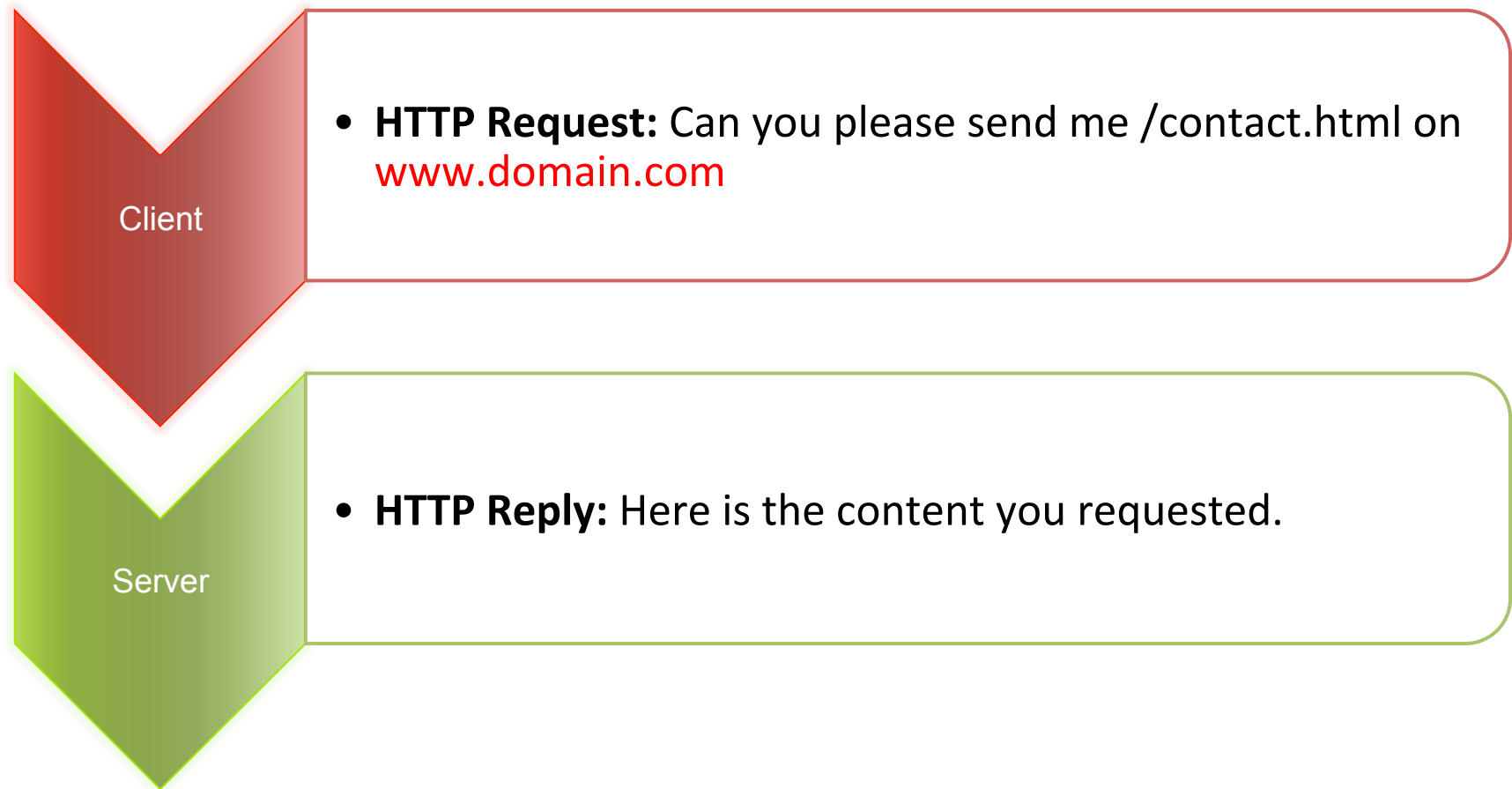
**Each SSL Certificate needs its own IP**



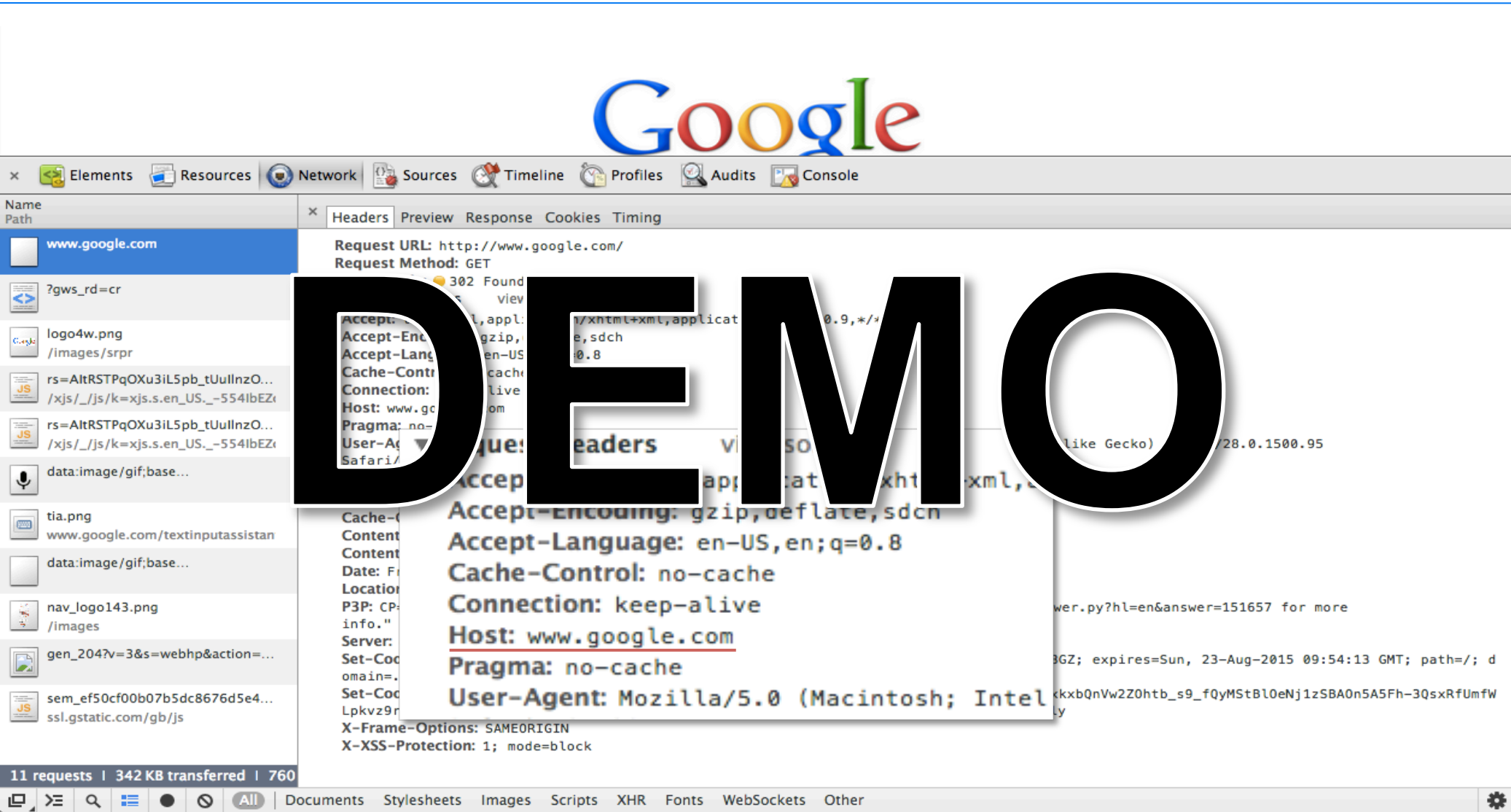


# Why do I need a dedicated IP address?

# Request on a non-secure connection

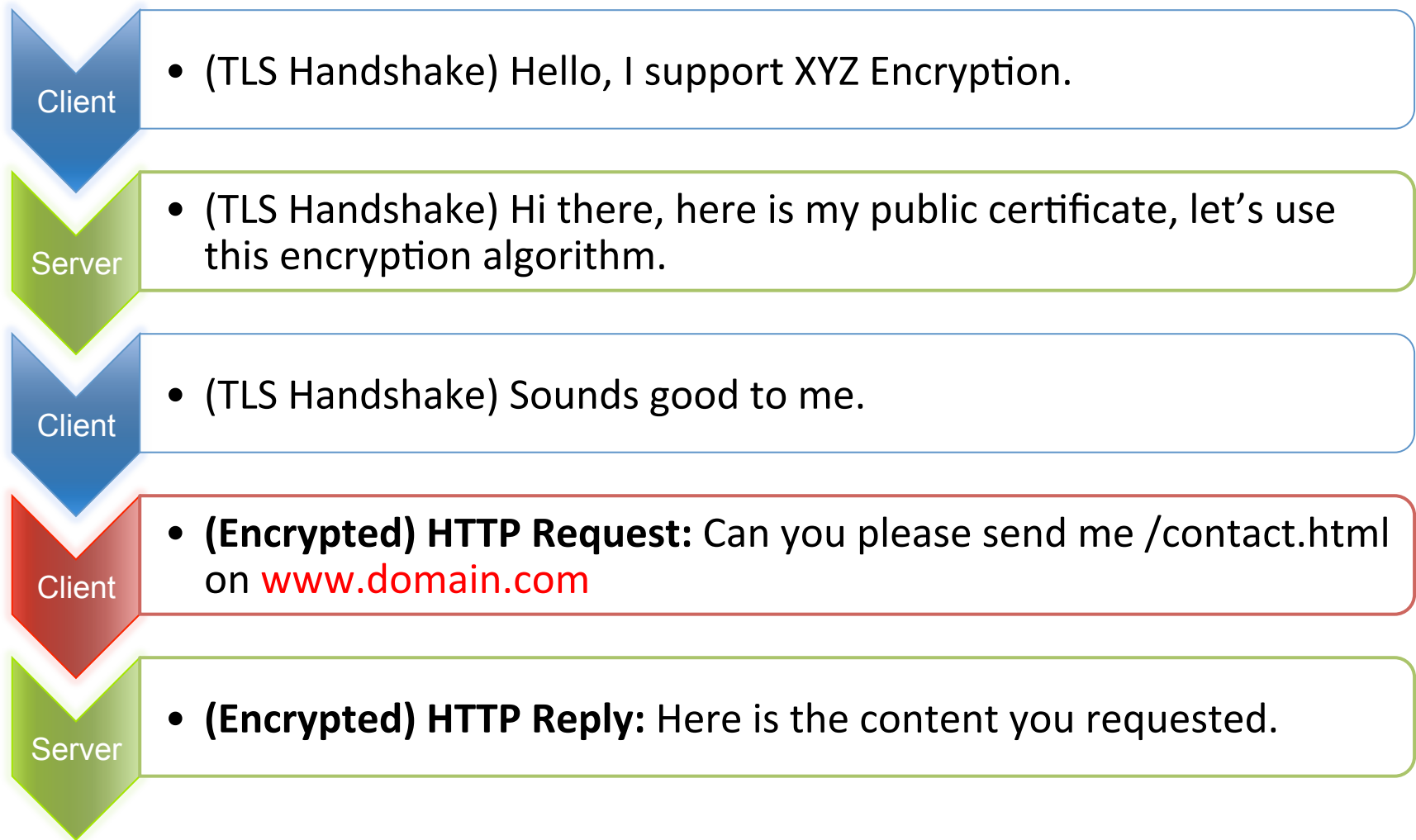


# Host: www.domain.com

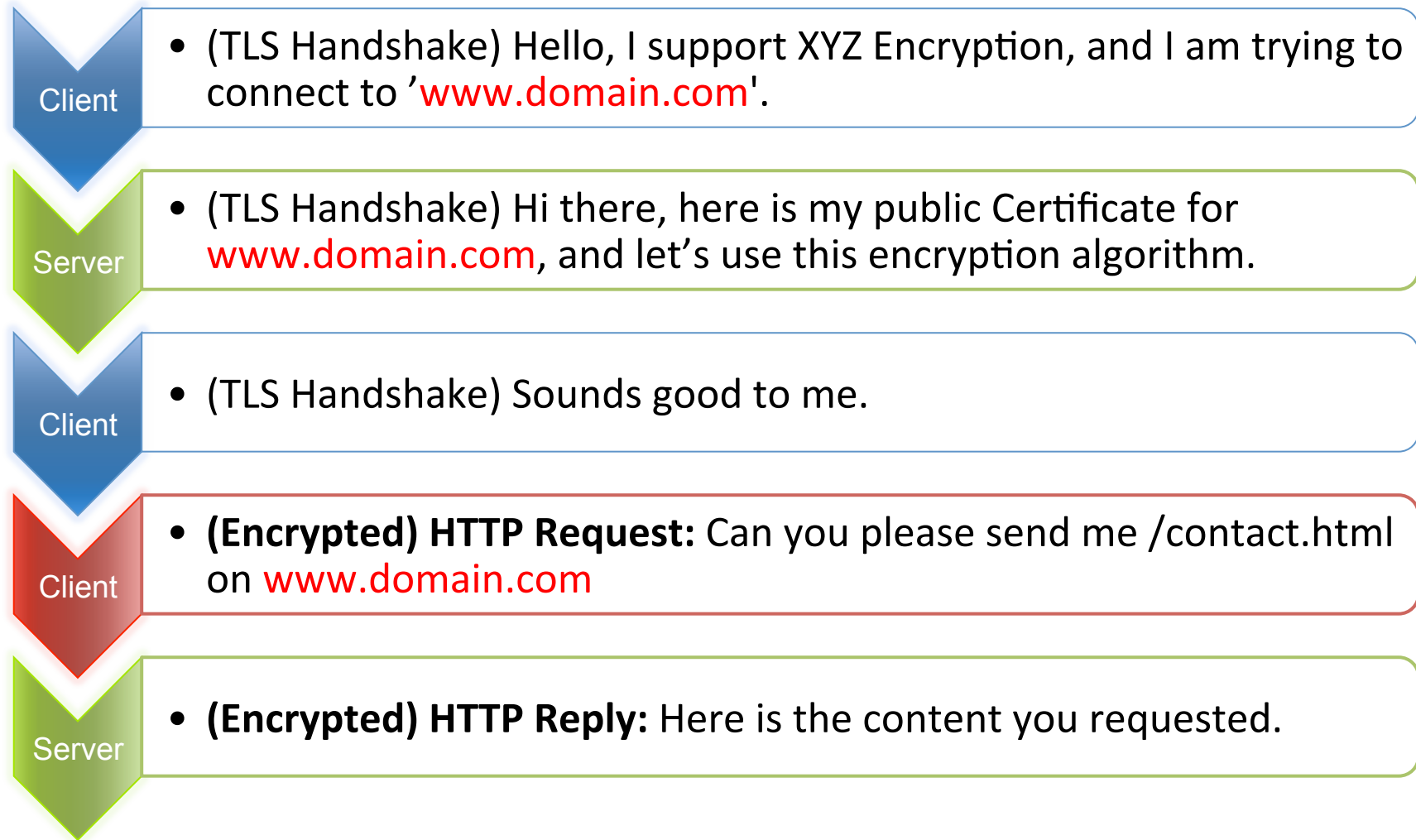




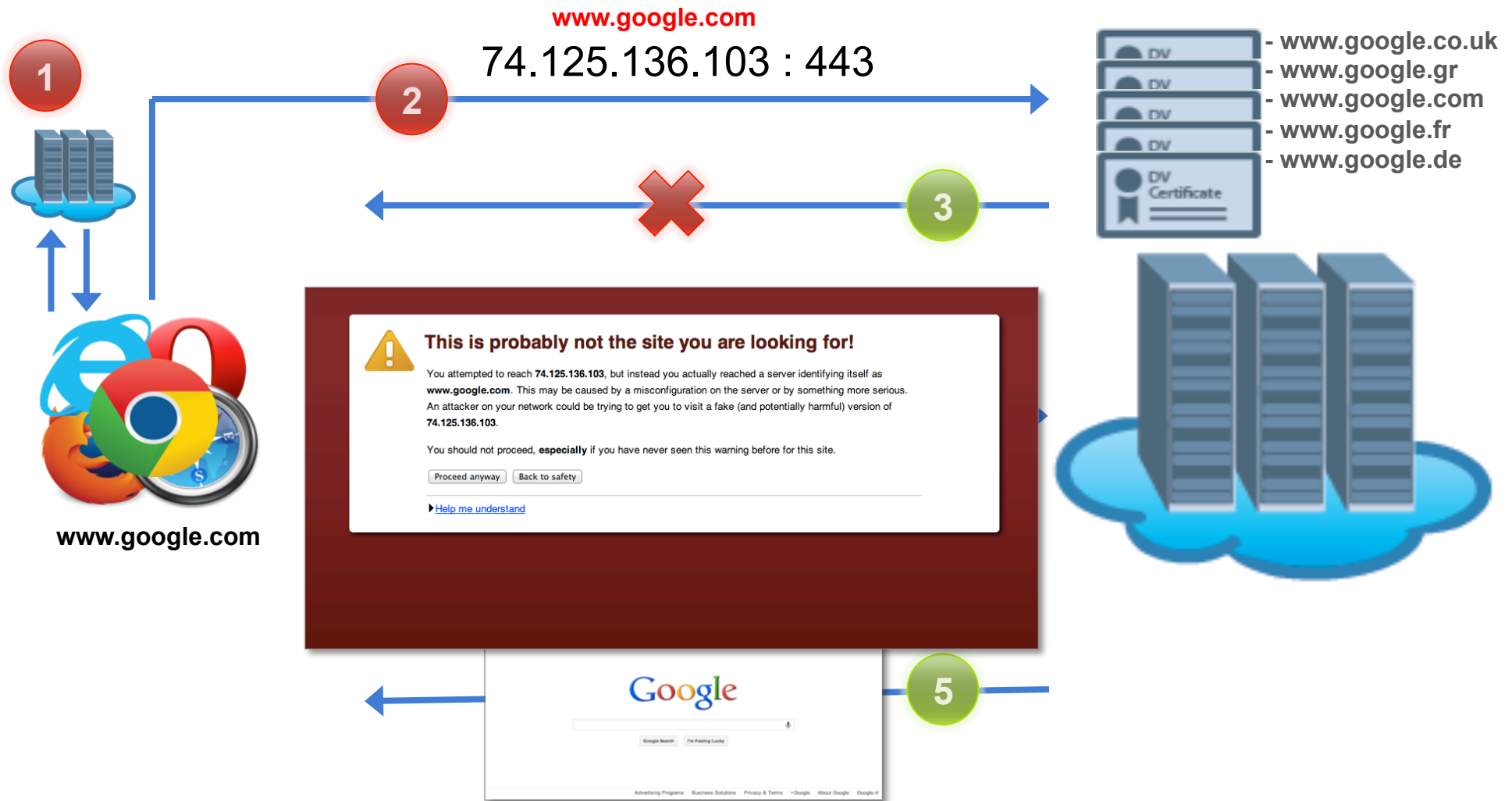
# Request on a secure connection



# 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 1.0 (0x0302)

#### ▶ Random

Session ID Length: 0

Cipher Suites Length: 72

#### ▶ Cipher Suites

Compression Methods: 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

### ▼ 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

# DEMO



# 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





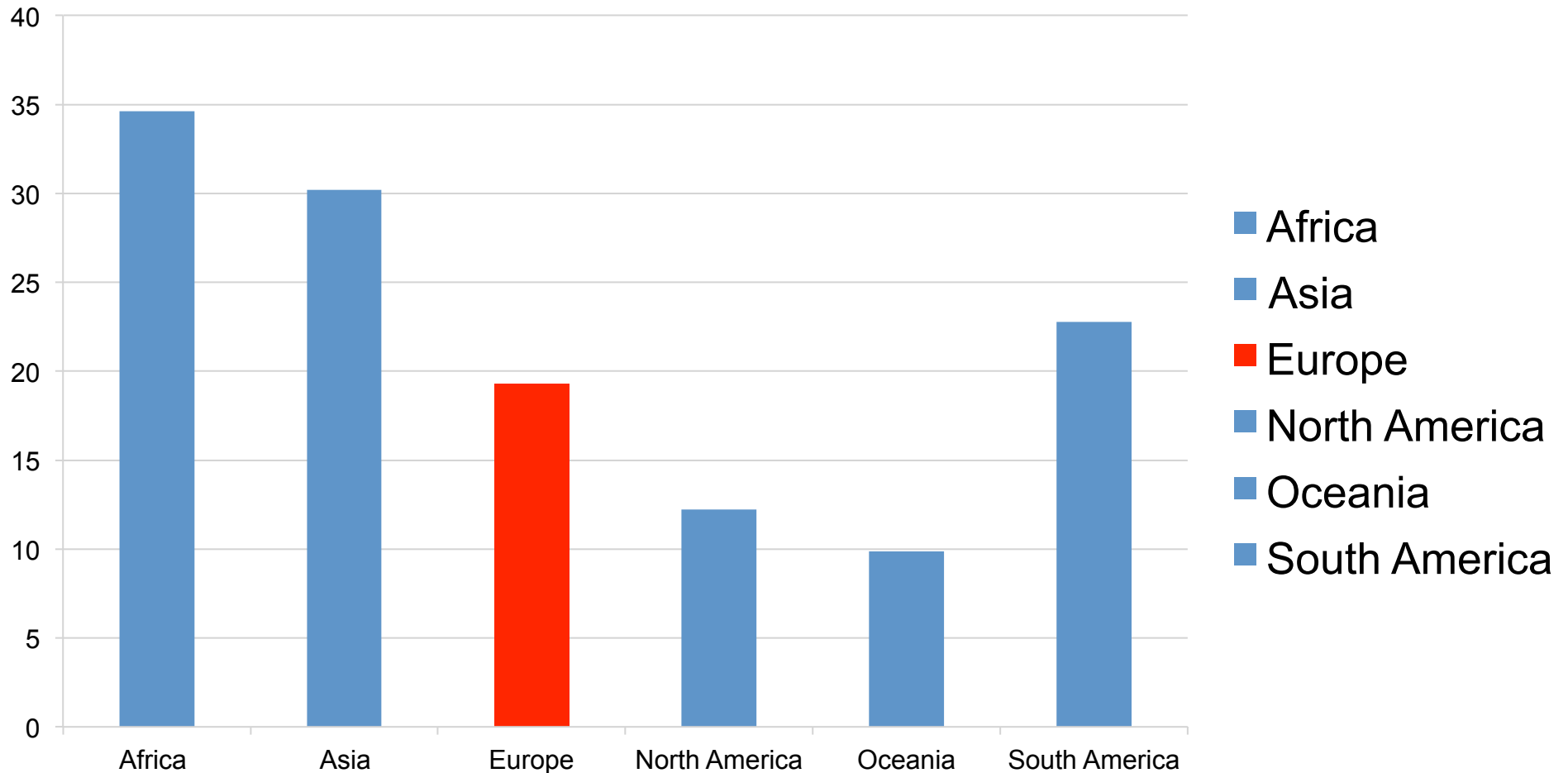
# Windows XP with SNI

---

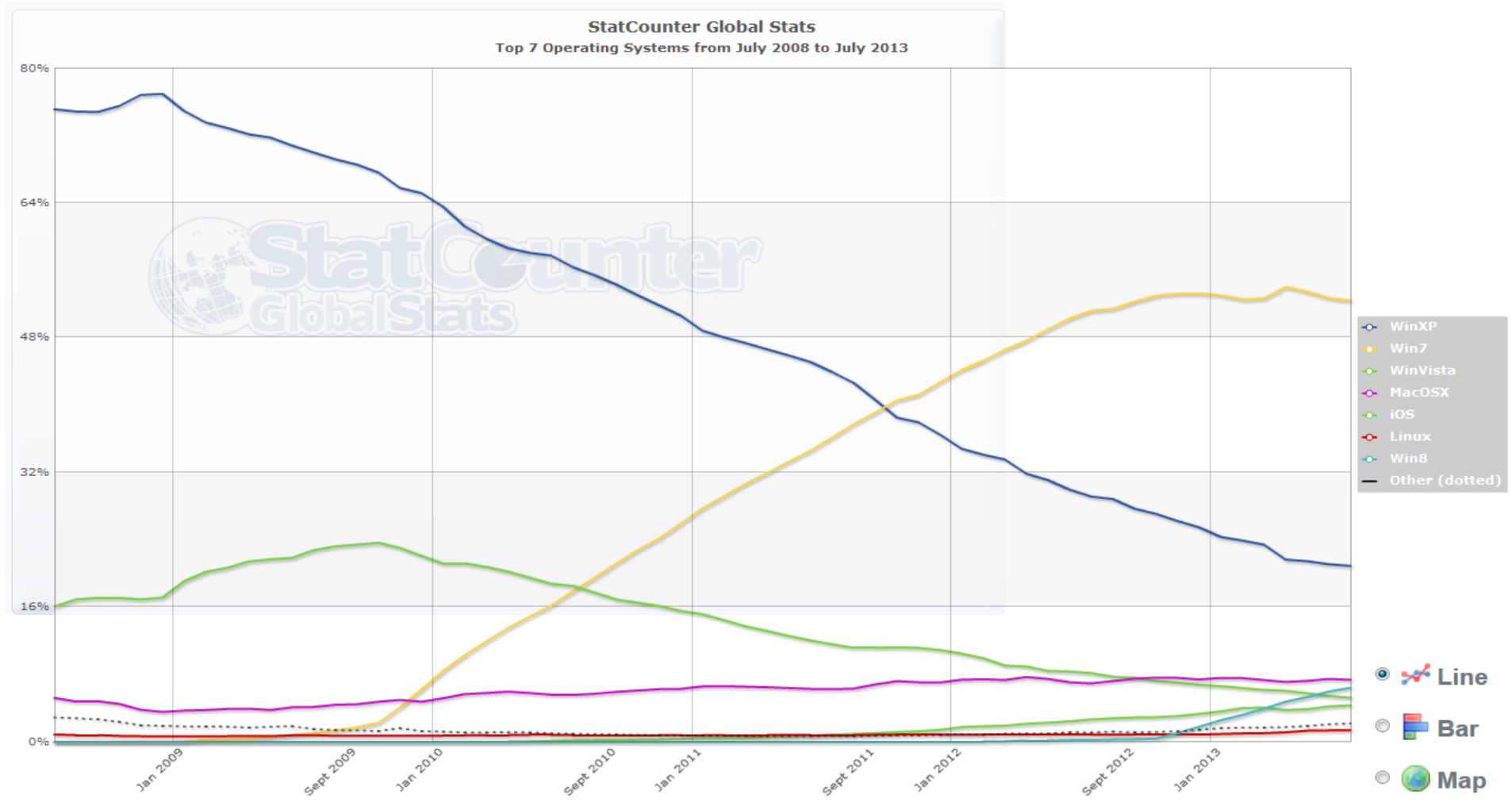
# DEMO

# Operating System Usage - Win XP – per continent

WinXP usage (July 2013)

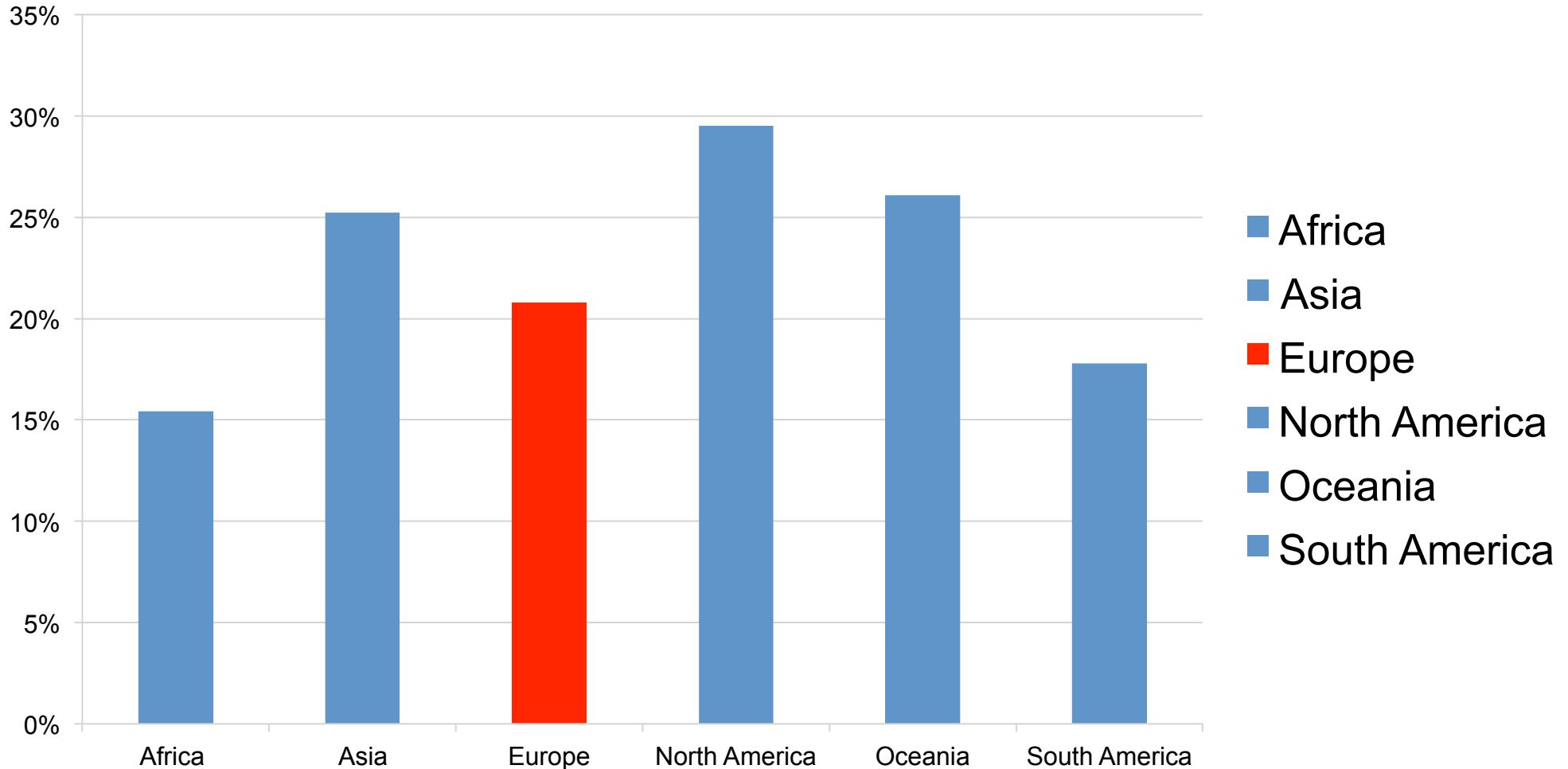


# Worldwide Operating System Usage - Win XP: 21%

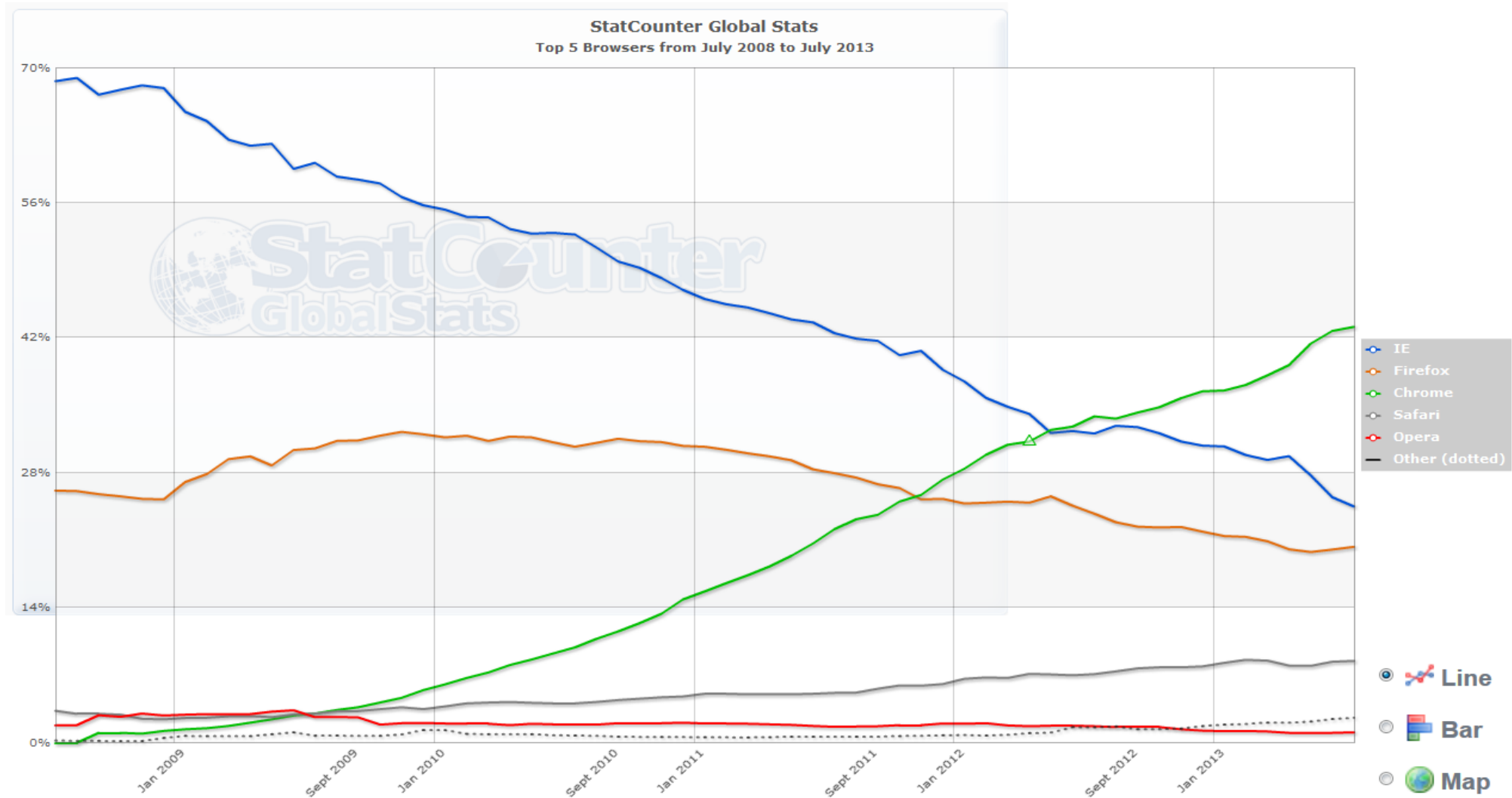


# Internet Explorer market share – Per continent

IE market share (July 2013)



# 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?

[Sign in](#)[Home](#)[Products](#)[Events](#)[Showcase](#)[Live](#)[Groups](#)[Google App Engine](#)[Feedback on this document](#)[Admin Console](#)[System Status](#)[FAQ](#)[Downloads](#)[▶ Getting Started](#)[▶ Java](#)[▶ Python](#)[▶ Go Experimental](#)[▼ Managing Your App](#)[▶ Admin Console](#)[Quotas](#)[Billing](#)[SSL](#)

## 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.



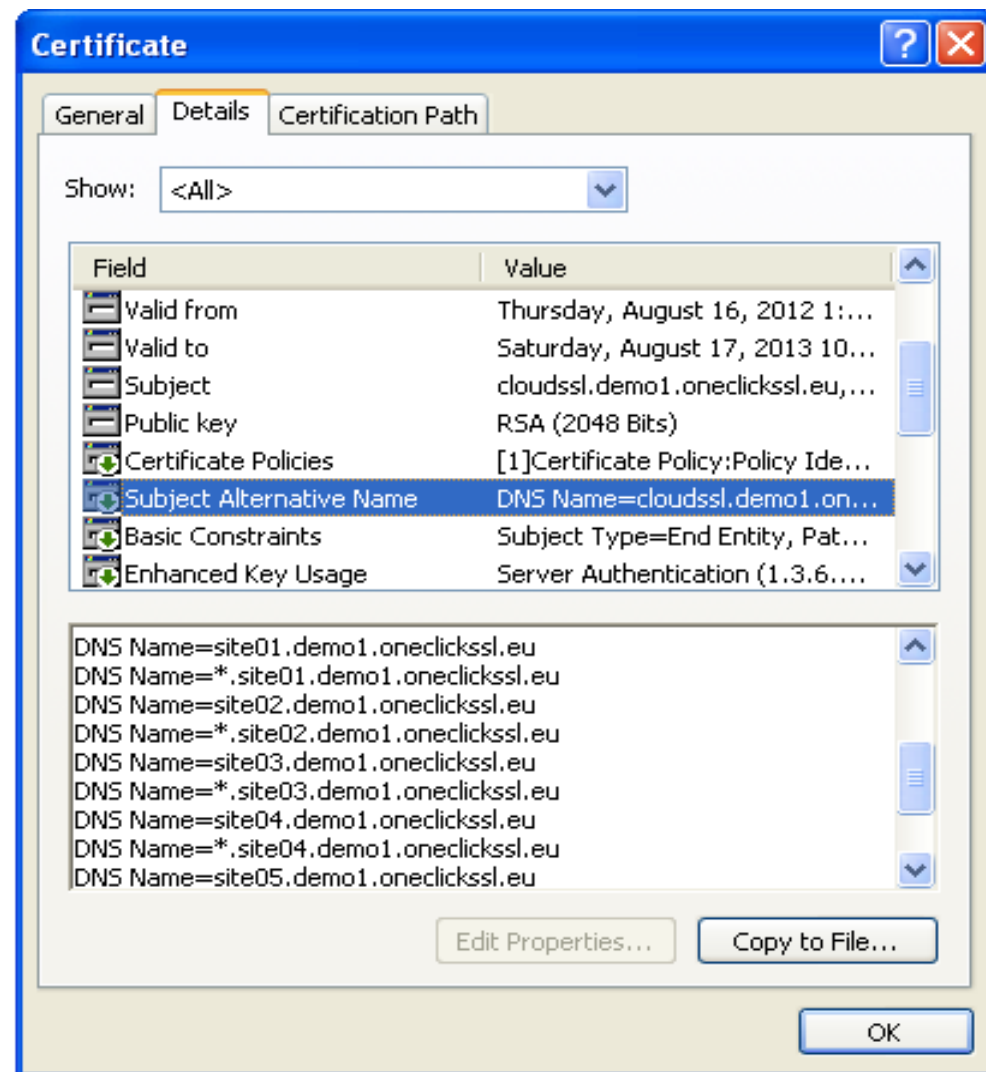
Authentication. Security. Trust.

[www.globalsign.com](http://www.globalsign.com)

# 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

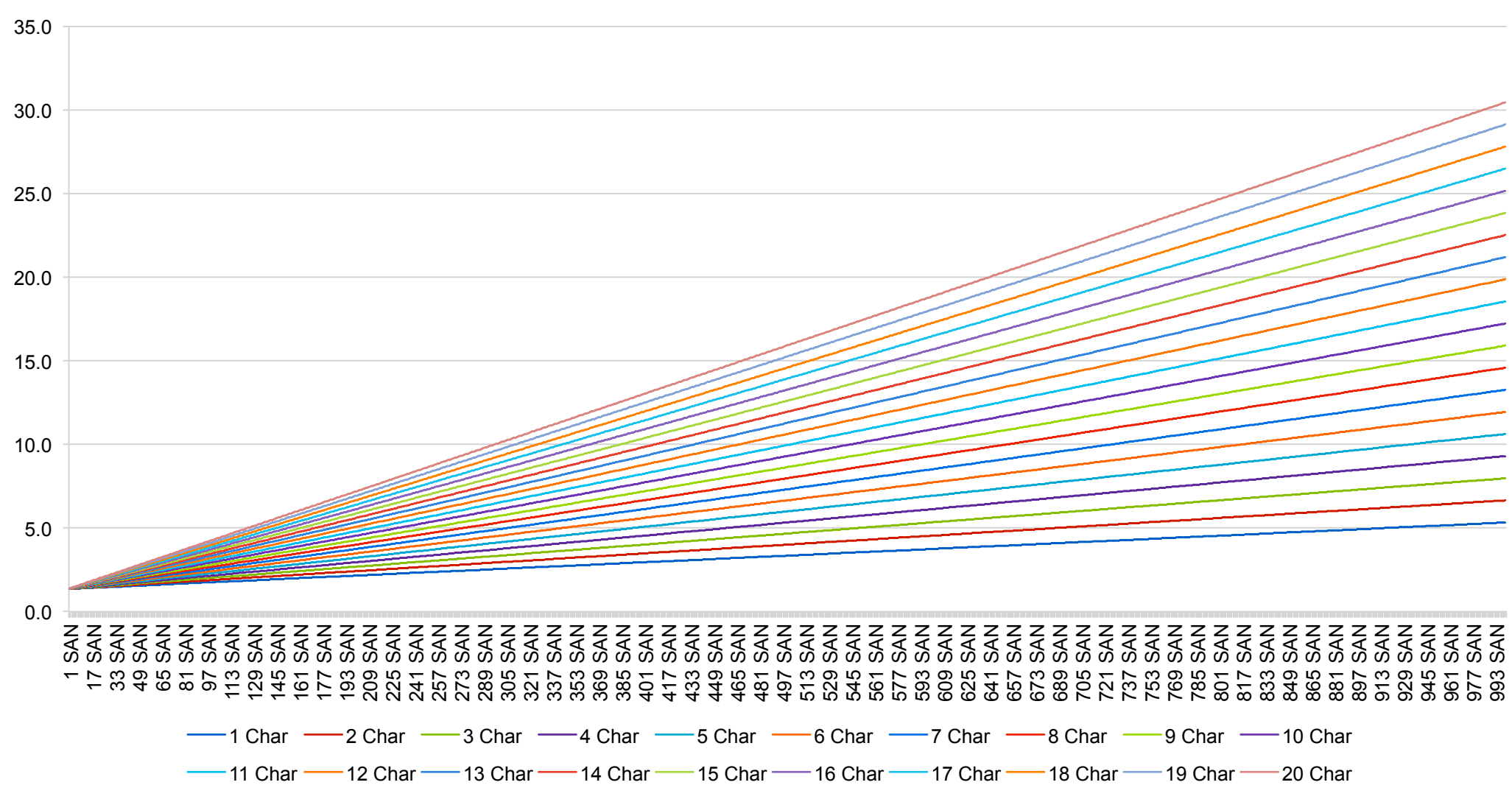
- Test results based on number of SANs and characters
- Note: Average number of characters in a domain – 13/14\*

\*Source: Nominet

- Certificate size limit is browser dependent

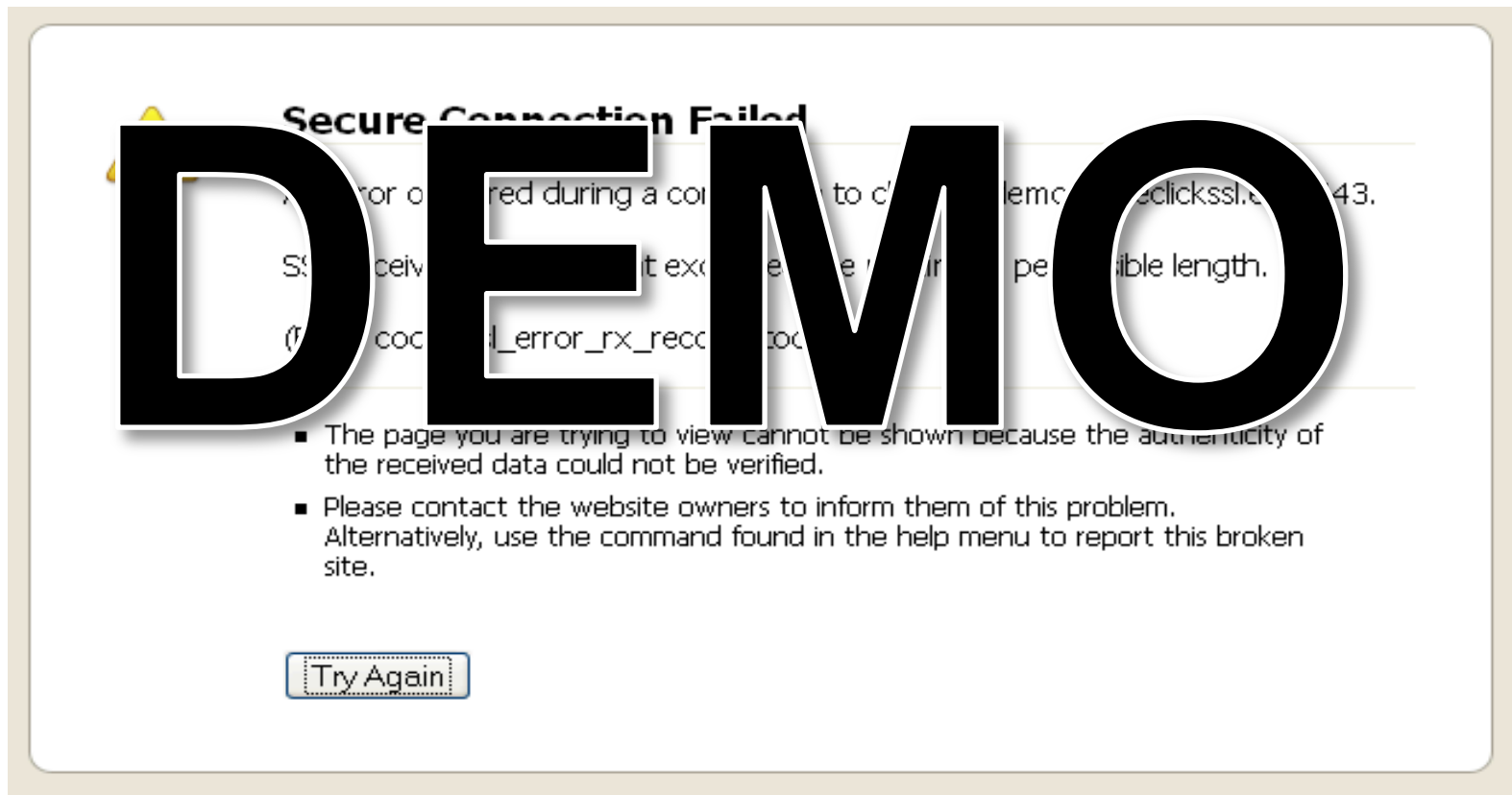


# Certificate Growth



# Maximum Certificate Size

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



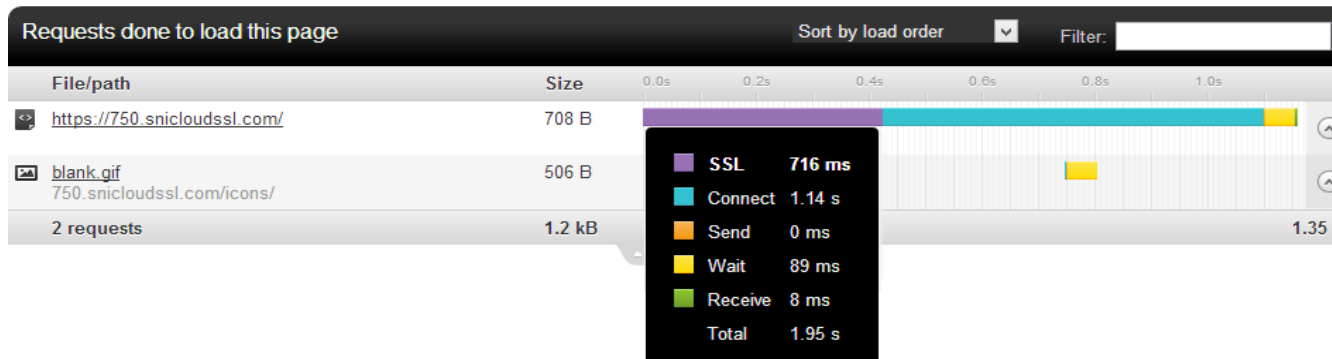


# Maximum Certificate Size

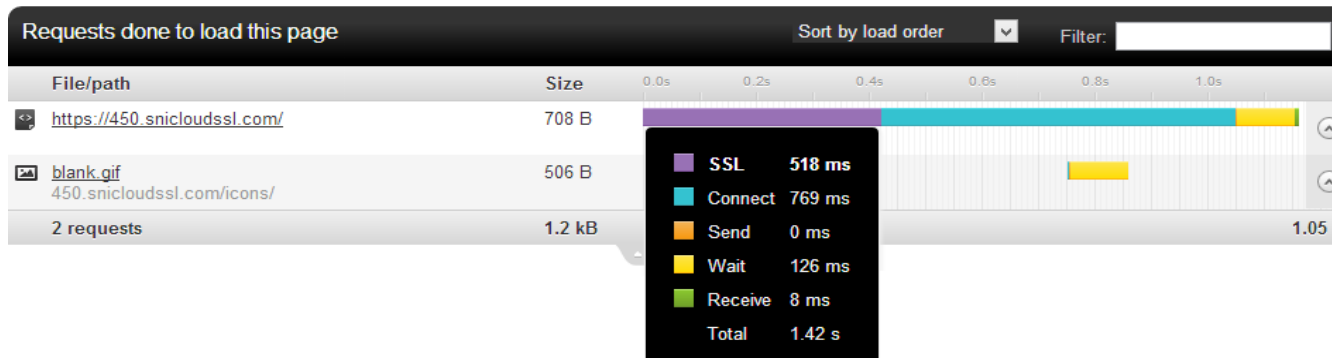


- Internet Explorer on Windows XP SP3 till Windows 7 has a certificate size limit of 44k.
- Windows XP without any service packs is limited to 22k.
- An average OCSP stapling response is about 1k
- Other TLS overhead is about 0.5k

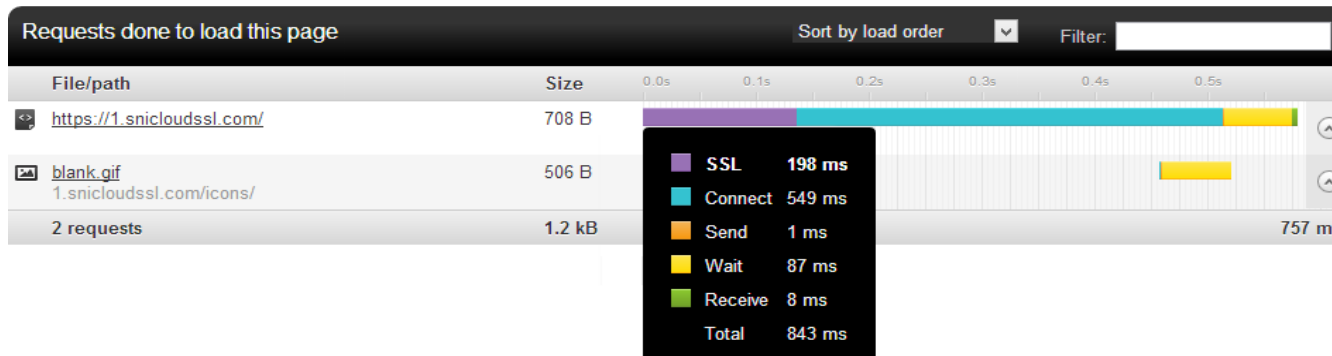
# Performance of multi-domain certificates



- 750 names:  
**716 ms**



- 450 names:  
**518 ms**



- 1 name:  
**198 ms**

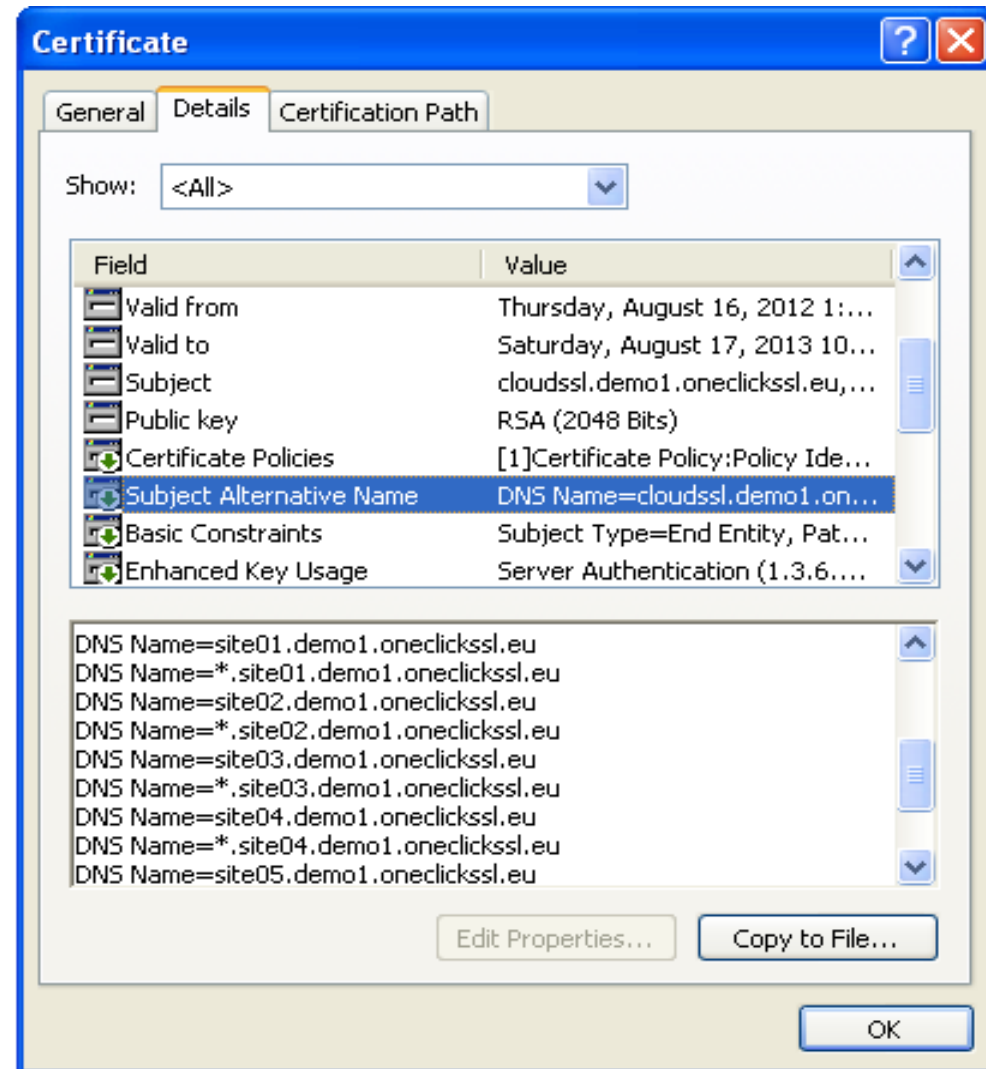


**Every 100ms delay  
costs 1% of sales**

**amazon.com<sup>®</sup>**

# 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)



---

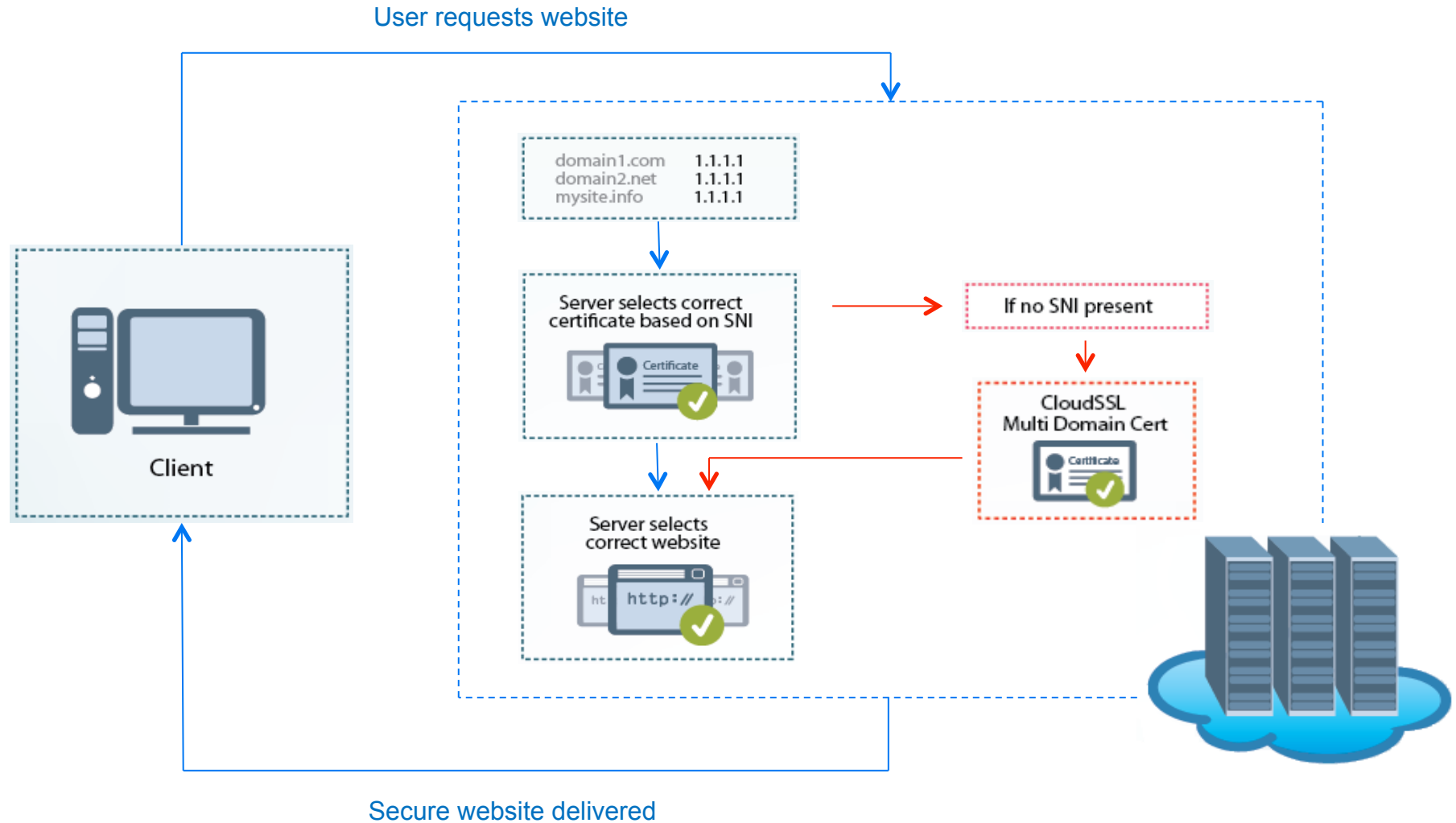
# What if we could use the best of both solutions?

**92% SNI**  
/ 8% CloudSSL

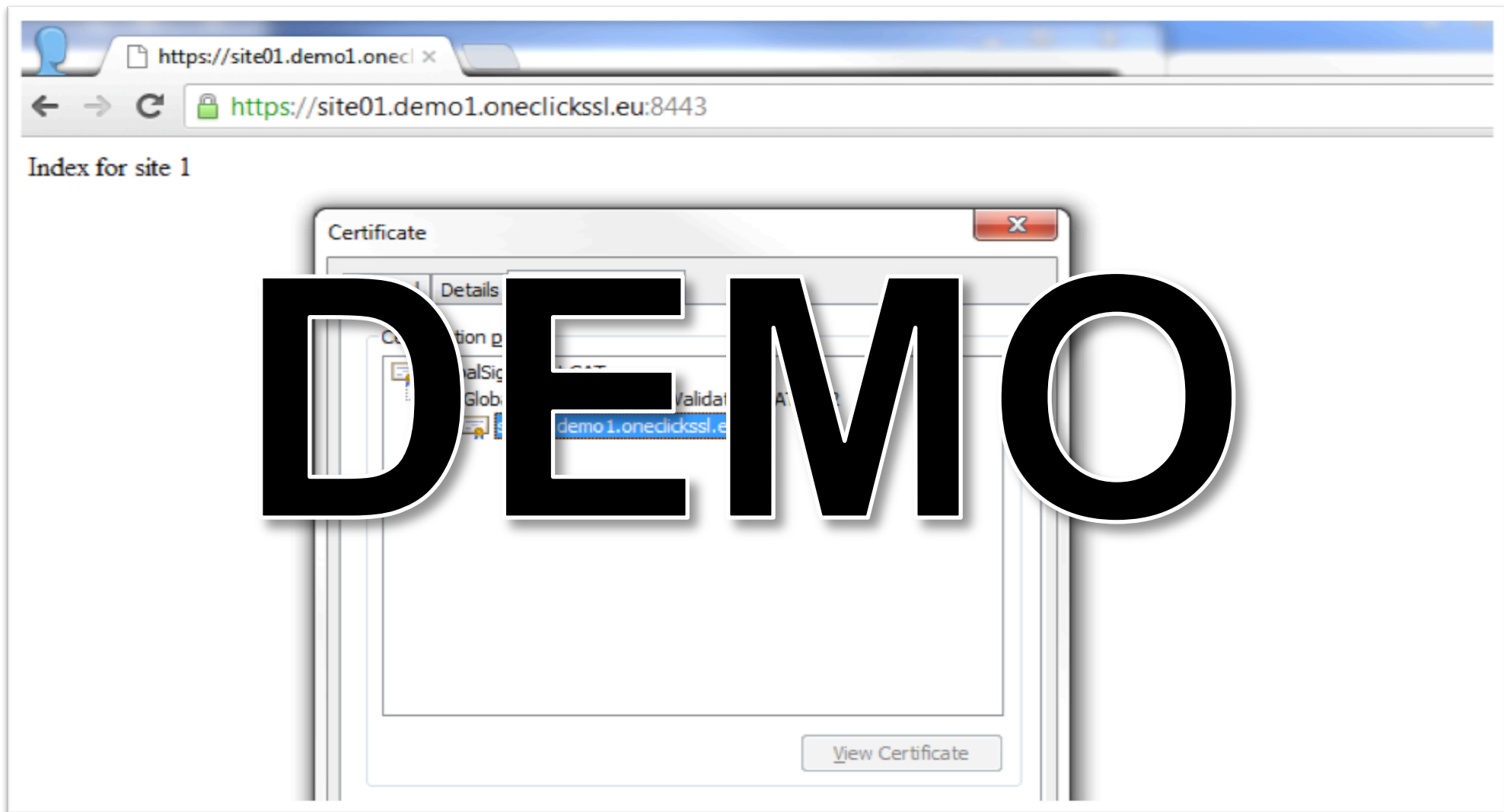




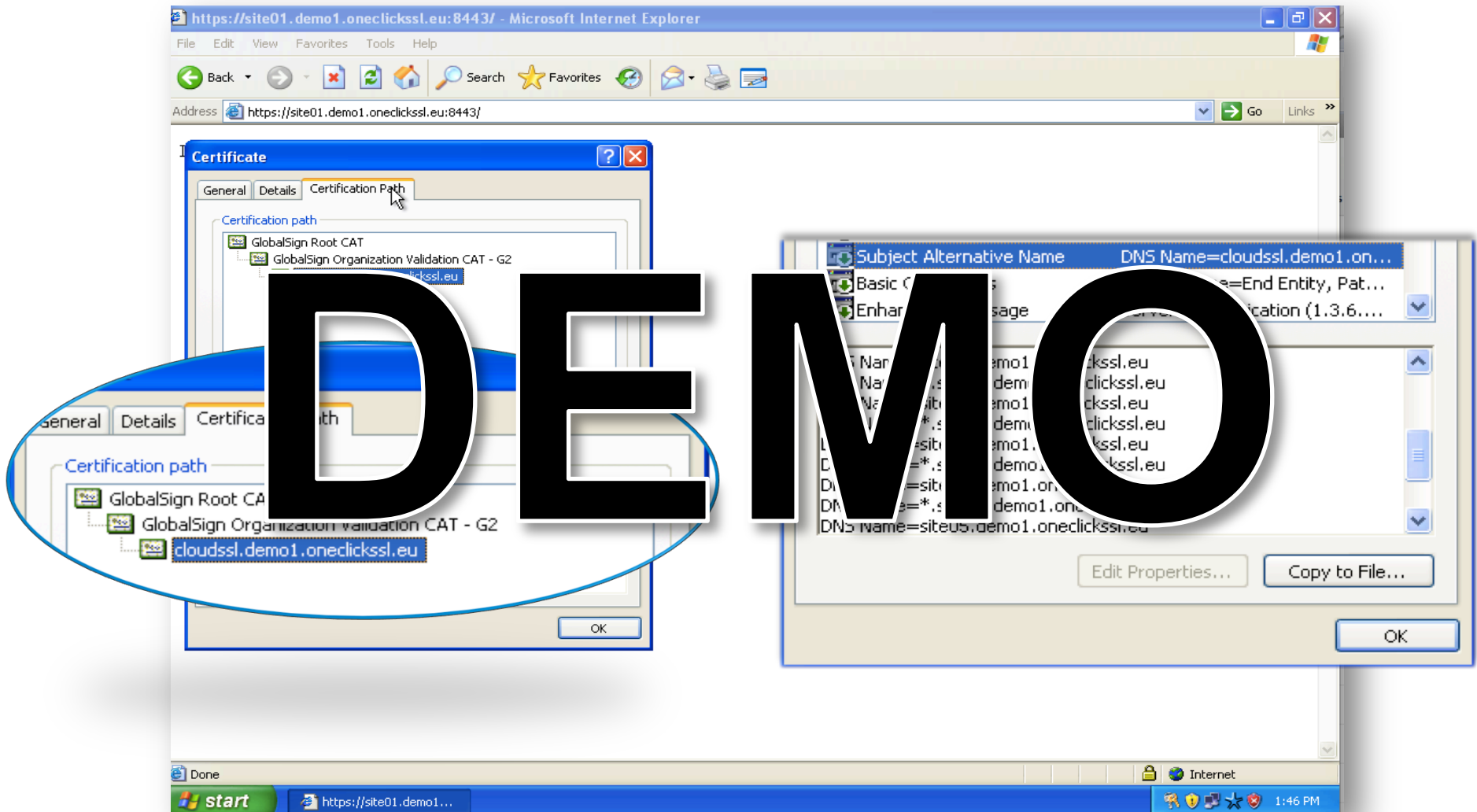
# SNI combined with CloudSSL



# 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

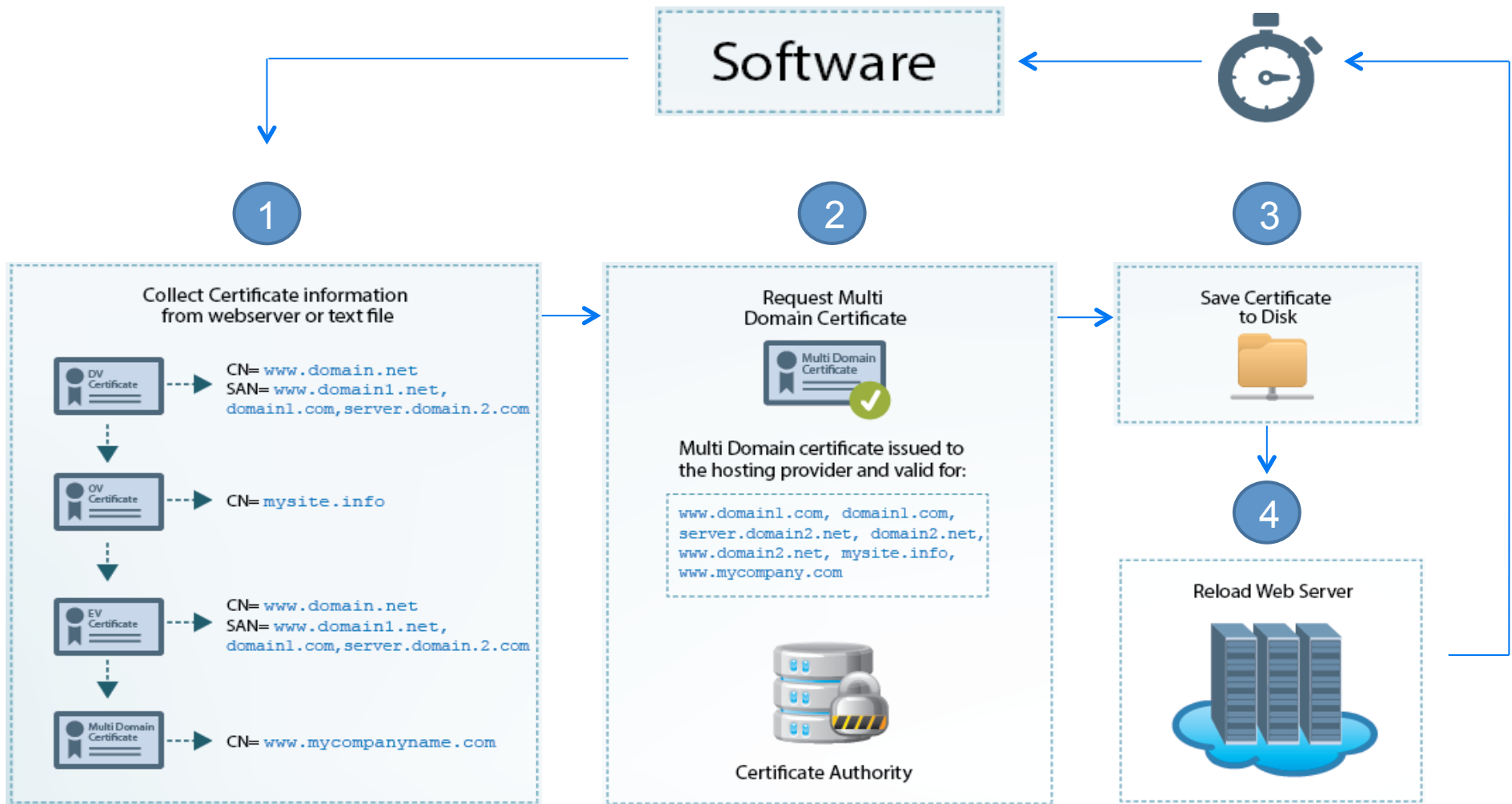


NGINX



Apache

# How does it work?





# Lets create a few sites in DirectAdmin

---

# DEMO

# Completely Automated Process



```
2013/03/11 14:15:01 SNI/CloudSSL version 0.8 (linux-386)
2013/03/11 14:15:03 Processing virtual hosts on: 192.168.1.7:443
2013/03/11 14:15:03 Adding check for: server231.snicloudssl.com
2013/03/11 14:15:03 Adding check for: www.domain.demo1.oneclickssl.eu
2013/03/11 14:15:03 Adding check for: www.demo.snicloudssl.com
2013/03/11 14:15:03 Adding check for: www.sameip.snicloudssl.com
2013/03/11 14:15:03 Adding check for: www.site2.demo1.oneclickssl.eu
2013/03/11 14:15:03 Adding check for: www.site3.demo1.oneclickssl.eu
2013/03/11 14:15:03 Adding check for: www.sni.demo1.oneclickssl.eu
2013/03/11 14:15:03 Adding check for: www.sni.snicloudssl.com
2013/03/11 14:15:03 Adding check for: www.sni2.demo1.oneclickssl.eu
2013/03/11 14:15:03 Retrieving certificates for order
2013/03/11 14:15:06 Starting check for: server231.snicloudssl.com
2013/03/11 14:15:07 Requesting certificate update
2013/03/11 14:15:41 Verifying domain control for 14 name(s)
2013/03/11 14:15:57 Not requesting a renewal, this certificate will expire in 356 days.
2013/03/11 14:15:57 Requesting a re-issue of the certificate
2013/03/11 14:16:10 Certificate updated and saved to disk
2013/03/11 14:16:10 Reloading Apache HTTP Server
root@oneclickssldemo2:/opt/snicloudssl#
```

# Automated domain control validation

---

# User Agent Redirect



## Apache

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

## NGINX

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

location /gsccloudsslvalidaion {
    alias /opt/sonicloudssl/html/;
}
```



# Same site, Different content

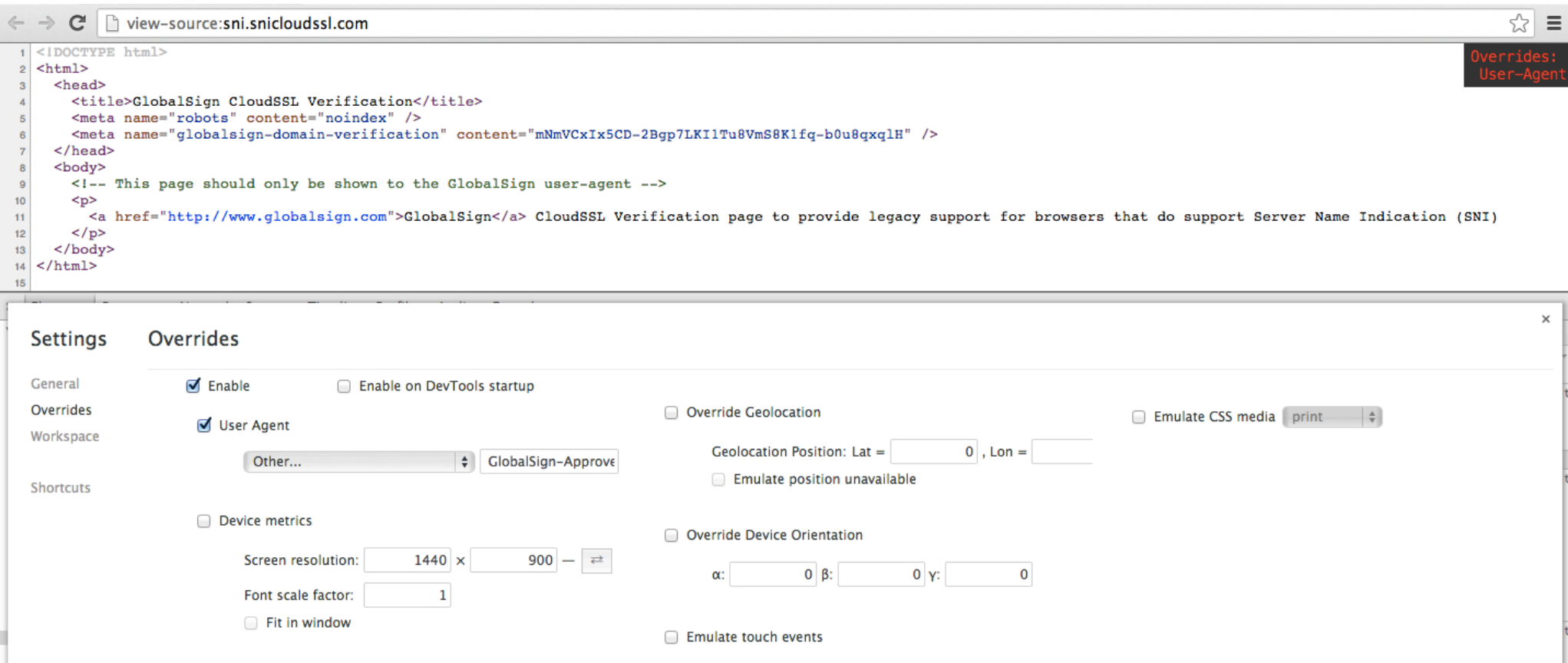
The image shows two browser windows side-by-side, illustrating how the same website can display different content based on the user agent string.

**Left Window:** The address bar shows `sni.snicloudssl.com`. The page content is a welcome message for `demo10.snicloudssl.com`, instructing the user to upload their website into the `public_html` directory. It includes a logo and a date created: `Thu Oct 10 15:00:41 2013`.

**Right Window:** The address bar shows `www.snicloudssl.com`. The page content is a `GlobalSign CloudSSL Verification` page, providing legacy support for browsers that do not support Name Indication (SNI). A red box highlights the `Overrides: User-Agent` setting in the DevTools console.

**DevTools Overrides Panel:** The bottom of the image shows the DevTools Overrides panel for both windows. The left panel shows the `Overrides` section with `User Agent` disabled. The right panel shows the `Overrides` section with `User Agent` enabled, and the `Other...` dropdown set to `GlobalSign-Approve`.

# Using meta-tag authentication



The screenshot displays a web browser window with the address bar showing `view-source:sni.snicloudssl.com`. The source code of the page is visible, showing an HTML document with a title "GlobalSign CloudSSL Verification" and meta tags for robots and domain verification. A comment in the body states: `<!-- This page should only be shown to the GlobalSign user-agent -->`. Below the source code, the Chrome DevTools "Overrides" panel is open, showing the "User Agent" override set to "GlobalSign-Approve".

**Source Code:**

```
1 <!DOCTYPE html>
2 <html>
3   <head>
4     <title>GlobalSign CloudSSL Verification</title>
5     <meta name="robots" content="noindex" />
6     <meta name="globalsign-domain-verification" content="mNmVCxIx5CD-2Bgp7LKI1Tu8VmS8K1fq-b0u8qxqlH" />
7   </head>
8   <body>
9     <!-- This page should only be shown to the GlobalSign user-agent -->
10    <p>
11      <a href="http://www.globalsign.com">GlobalSign</a> CloudSSL Verification page to provide legacy support for browsers that do support Server Name Indication (SNI)
12    </p>
13  </body>
14 </html>
15
```

**Overrides Panel:**

- General:** ☒ Enable, ☐ Enable on DevTools startup
- Overrides:** ☒ User Agent, ☐ Override Geolocation, ☐ Emulate CSS media (print)
- Workspace:** Other... (dropdown), GlobalSign-Approve (text input)
- Shortcuts:** ☐ Device metrics, ☐ Override Device Orientation, ☐ Emulate touch events

**Device Metrics:** Screen resolution: 1440 x 900, Font scale factor: 1, ☐ Fit in window

**Device Orientation:**  $\alpha$ : 0,  $\beta$ : 0,  $\gamma$ : 0



# 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





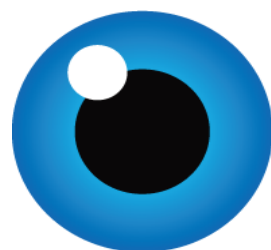
# Thank you

Paul van Brouwershaven

[paul.vanbrouwershaven@globalsign.com](mailto:paul.vanbrouwershaven@globalsign.com)



@vanbroup



**GlobalSign®**

