

GlobalSign OneClickSSL

From application to installation – fully automating SSL Certificate provisioning on IIS, Apache, Plesk and cPanel

GLOBALSIGN WHITE PAPER

Steve Roylance, Business Development Director
Steve Waite, Chief Marketing Officer

GMO GlobalSign Inc.



www.globalsign.com.sg
www.globalsign.com.au
hk.globalsign.com

CONTENTS

- Introduction..... 3
- How do the GlobalSign Security Services fit into hosting?..... 3
 - SSL Certificates..... 4
 - What is an SSL Certificate?..... 4
 - What is TLS? 5
- OneClickSSL Automation Technologies..... 6
 - Deployment & Automation – Traditional methods 6
 - Deployment & Automation - OneClickSSL 7
- Looking at The process in detail..... 8
 - Multi-factor Authentication with OneClickSSL..... 8
 - IIS 6, 7 and 7.5 oneclickssl.exe 9
- Benefits of Partnering with GlobalSign 11
 - Hosting Companies 11
 - Generate a new revenue stream / augment existing revenue stream 11
 - Reduce your Support Costs 11
- Partner Program Levels..... 12
- Why Partner with GlobalSign? 12
- Inquire about OneClickSSL & the Partner Program 13
- About GlobalSign 13

INTRODUCTION

A Secure Sockets Layer (SSL) Certificate coupled with the Transport Layer Security (TLS) protocol is no longer simply a means to obtain a 'padlock' within a browser secure session. With the majority of modern web browsers, identity information concerning the owner of the domain and their physical location is presented to the relying party in an enhanced interface. Protecting and securing credit card details is mandated by bodies such as the Payment Card Industry (PCI) and is therefore a minimum requirement to engage in e-Commerce on the Internet. Many other pure transactional and non-transactional data transfer types can now also be successfully protected. These typically include protection of additional credentials and personally identifiable information, which is sometimes requested when either logging on, or signing into a remote service. Any further additional authentication challenge/response questions should also be protected to the same degree as the username and password itself.

SSL Certificates have also found increasing levels of adoption in database to database communications and mail server to mail server connectivity as network boundaries become increasingly fragmented. However, although SSL Certificate usage has seen significant and diverse growth over many years, the SSL Certificate lifecycle itself has remained stagnated on first principles – generate a Certificate Signing Request (CSR), submit the CSR to a Certificate Authority (CA), be challenged for authority and vetted by a Registration Authority (RA), receive back the signed certificate, install the certificate and any associated intermediate issuing certificates and upon the eventual expiry, renew the certificate following the exact same process again. Furthermore and to complicate matters, the applicant is still assumed to be the administrator of the webserver, which with increasingly virtualized or outsourced hosting environments, often is not the case.

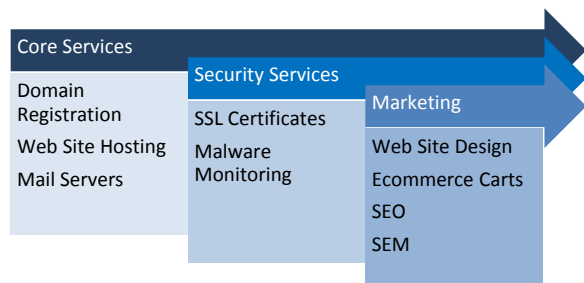
Building upon a decade of operational experience in issuing SSL certificates across a diverse customer base, GlobalSign has designed, developed and now patented OneClickSSL™ - A radical change in workflow practices to dramatically improve the traditional SSL provisioning process. Rather than expect users to understand and

follow the usual lifecycle, OneClickSSL simplifies the process from application to installation with levels of automation previously considered impossible – significantly boosting efficiency whilst at the same time increasing security. OneClickSSL is delivered via a simple client plug-ins for Microsoft IIS (6+), Linux based Apache implementations and also for the cPanel and Parallels Plesk control panels.

This white paper explains the basics behind SSL certificates and TLS encryption and highlights how GlobalSign's OneClickSSL provisioning technology works, its use case and its necessity for today's disparate network architectures. In addition the paper initially looks at the sales opportunities for hosting companies and advises how to fit the services into existing hosting portfolios as well as providing details on how provisioning SSL certificates can be fully automated.

HOW DO THE GLOBALSIGN SECURITY SERVICES FIT INTO HOSTING?

Many hosting companies that find they are already hosting hundreds of SSL Certificates and are now recognizing the potential for revenue gains by increasing their average customer values through providing SSL Certificates as an authorized reseller. Hosting companies who offer SSL Certificates in their hosting packages or as a value-add option gain the immediate benefits of increased revenues and a more complete and "sticky" product portfolio.



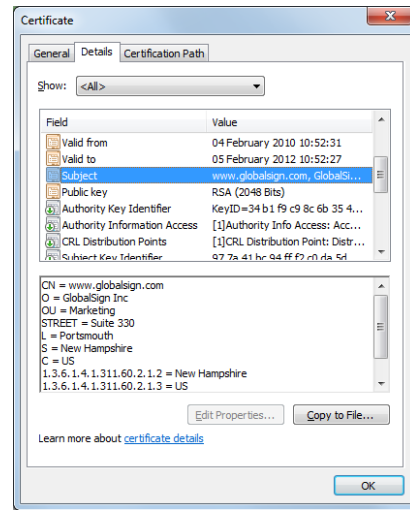
The diagram shows a high level view of the value chain for hosting. Security services can easily be added as a value-add to all hosting bundles, or sold separately as an individual line item. As Security Services support the Core

Services, the customer profile to Core Services is essentially identical.

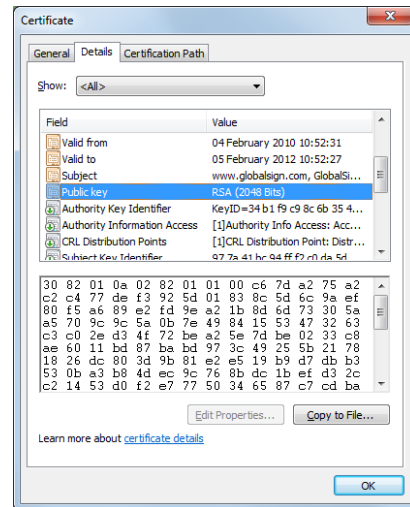
SSL Certificates

What is an SSL Certificate?

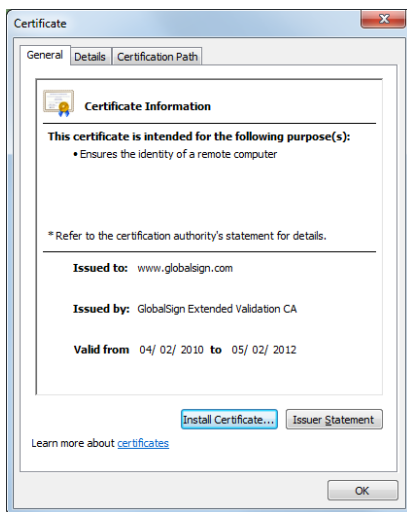
An SSL Certificate is a small, internationally recognized (typically RFC5280 (Request For Comment)) file type, usually formatted as an x.509 version 3 format file. In its most basic form it contains both a ‘public’ key (a very big number which is fine to share with other parties) and some information about the owner of a matching ‘private’ key (another very big number that must be kept secret/private). A combination of these public and private keys allows the certificate to be used to create digital signatures and verify them. In fact a certificate is simply a way to securely transport the owner’s public key around as it’s secured within the file by a signature from the matching private key. There are various forms of accepted cryptography techniques available that can be used to create the public and private key pairs. The most popular at the moment is RSA (named after the people who first publically described the methods - Rivest, Shamir and Adleman) with ECC (Elliptic Curve Cryptography) due to supersede RSA in the coming years due to its speed and equal security with a smaller key size. This white paper will not dive into the full details of PKI (Public Key Infrastructure) as it is beyond its scope.



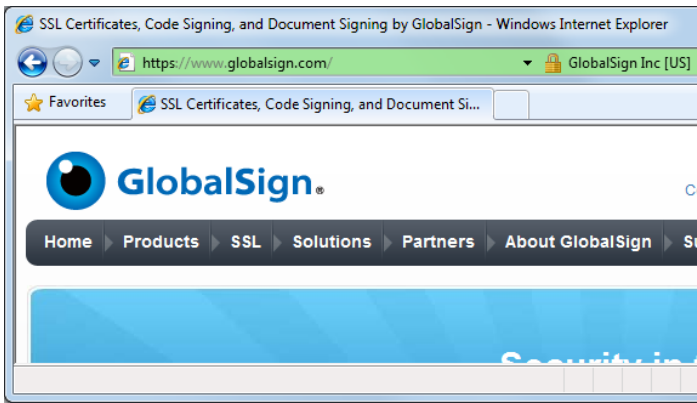
Details about the owner (Subject)



The owners public key (2048 bit)



An 'ExtendedSSL' for www.globalsign.com



The resulting web site as rendered with IE 7, which highlights the owner's name to relying parties by extracting it from the OrganizationName within the Subject

What is TLS?

The Transport Layer Security (TLS) protocol is the most widely deployed security protocol used today and follows on from the previous versions of the SSL protocol. (SSL Certificates have typically maintained their naming convention rather than being referred to as TLS Certificates). It is essentially a protocol that provides a secure channel between two machines operating over the Internet or an internal network. In today's Internet focused world, we typically see TLS in use when a web browser needs to securely connect to a web server over an unsecure channel (i.e. typically the Internet).

http://en.wikipedia.org/wiki/Transport_Layer_Security offers an in-depth view of the TLS protocol, however in simple terms it can be seen as a secure exchange of secret numbers. Once the numbers have been exchanged then all packets of data can be encrypted with the secret number. (The secret number is often referred to as a session key and is typically a 256 bit symmetric key). An SSL Certificate is used to convey the identity of the server and its public key to the relying party in a secure way so that the relying party can trust that they are indeed talking to the domain they intended. After a handshake where cryptographic capabilities of server and browser are compared, the relying party is able to verify the identity of the server by encrypting a challenge with the servers' public key from the SSL Certificate. Certification Authorities add value to the data exchange between the two parties by attesting to the authenticity of the SSL Certificate and therefore its public key, by signing it with a

signature that the browser itself recognizes. This is why Certification Authorities are often referred to as 'Trusted Third Parties'.

Technically TLS is a transparent protocol, which requires little interaction from the end user when establishing a secure session. In the case of a browser, users are alerted to the presence of SSL when the browser displays a padlock, or in the case of Extended Validation SSL the browser address bar displays both a padlock and a green bar. This is the key to the success of SSL/TLS – it is incredibly simple experience for end users.

SSL Certificate are typically seen by end customers as padlocks: note the lack of anything "Certificate" related; they just simply see the https and the padlock. "Secure Sites" are what customers look for, not SSL Certificates!



ONECLICKSSL AUTOMATION TECHNOLOGIES

Deployment & Automation – Traditional methods

SSL Certificates are created following a lifecycle model that can be typically segmented into 6 stages. A poorly optimized lifecycle will put undue pressure on support staff through increased levels of phone calls and emails to solve technical issues as the underlying technology itself is complex and therefore mistakes can be made.

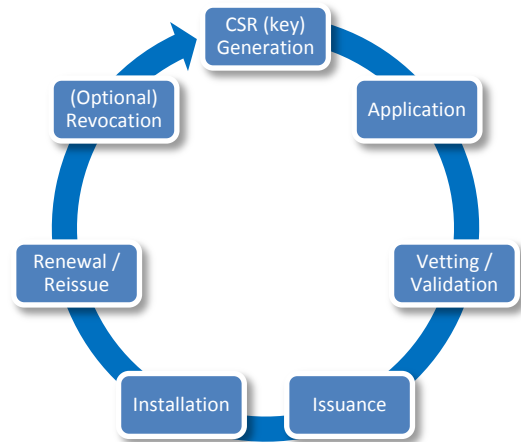
Administrators prior to OneClickSSL needed a relatively good level of understanding of cryptographic key management principles and processes in order to not only manage SSL deployments, but more importantly to know why they failed at any particular point.

To adequately protect the organization’s SSL secured servers, Admins must have a good understanding of:

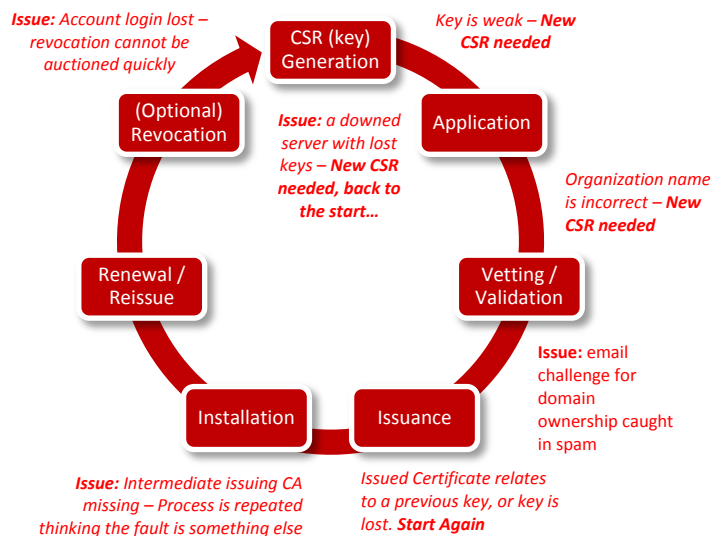
- **Cryptographic key sizes:** when generating Certificate Signing Requests (CSRs), the admin must ensure that a suitable key size is used – for example 2048 bit is now recommended by NIST (National Institute of Science & Technology) and also best practice for many of the browser specific root programs, yet few admins in the Enterprise and Hosting environments are familiar with this recommendation and may unnecessarily expose their organizations through the reliance upon a weak key.
- **Algorithms:** when generating CSRs, administrators must ensure that the correct asymmetric algorithms are used to generate the keys – again, assuming they are familiar with algorithm implementation and usage.
- **Intermediate issuing CA:** Many Certificate Authorities protect their root certificate in an offline environment choosing to issue SSL Certificates to domain owners from an intermediate CA. As such, the correct intermediate CA must be installed onto the web server for the full ‘chain’ to be seen by the browser during the negotiation phase. A broken or incomplete chain often results in the website being untrusted by the browser. Administrators must be familiar with where this intermediate certificate must be installed.

- **Incorrect Business Name:** The true and correct Business Name is not known by the administrator creating the CSR, meaning that the Certification Authority rejects the CSR midway through the process.
- **SPAM filter and lost e-mail delays:** the Administrator may receive an email challenge response from the CA to prove control of the domain. Loss of this email to a SPAM filter or an inability to receive emails causes the process to stop.

Traditional SSL Certificate provisioning:



The Problems of traditional SSL Certificate provisioning:



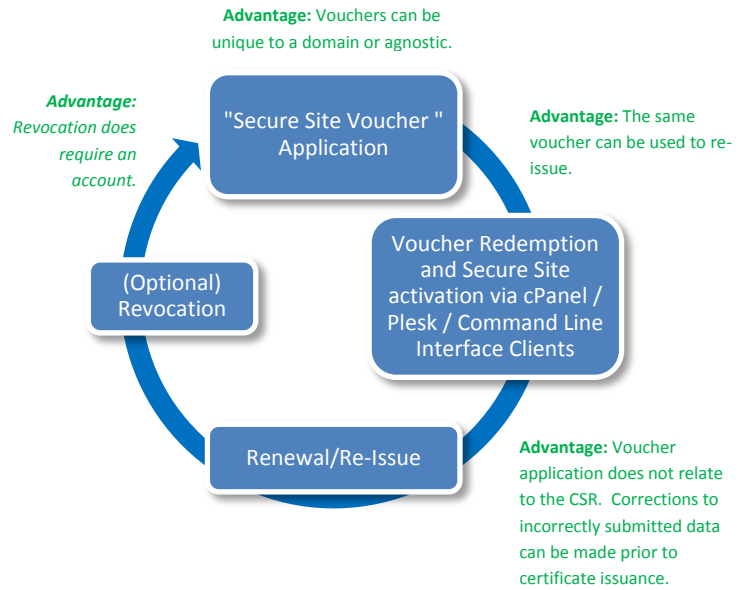
If the private key becomes compromised, the Administrator must understand how to revoke the certificate. Failure to revoke is a serious security threat as the holder of the compromised key is able to either spoof their identity to relying parties or eave drop on secure communications between parties. Few Administrators actually know the process of revoking the certificate with their SSL Provider and as the compromise can sometimes happen years after the issuance of the original certificate, the login details may have been lost or indeed the Administrator may have been replaced.

GlobalSign OneClickSSL rewrites the SSL paradigm and turns a high-tech complex lifecycle management overhead into a simple, low tech solution. This enables Administrators, or even non-Admins, to manage the entire SSL lifecycle with practically zero training requirements on cryptography, key size and algorithm selection and revocation. Neither does the Admin need to understand how and where to create CSRs, where to install issued Certificates and how to bind the issued certificates to the appropriate sites/locations.

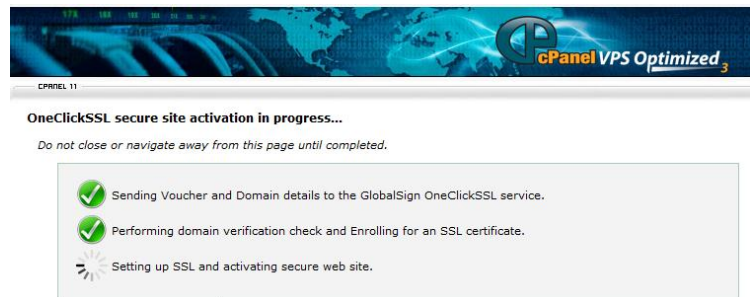
Deployment & Automation - OneClickSSL

OneClickSSL allows users to apply for "Secure Sites" and not to worry about certificate technology, CSRs and other complex cryptographic considerations. Rather than dealing in these terms, the site owner only needs to understand the term 'voucher'. A voucher can be thought of as an authentication token for issuance of an SSL certificate for a domain. If the voucher is linked to the details of the domain to be secured prior to use, then these additional details can be added to the certificate during the issuance process. This separation of the purchasing process and the enrolment/issuance process suits both the novice website administrator as well as enterprises which specifically allocate responsibility to different departments for each activity.

Certificate provisioning via OneClickSSL and some of its advantages:



With OneClickSSL, customers simply acquire a Secure Site "Voucher" and at a later date exchange the voucher for an SSL Certificate. This is done by using one of the OneClickSSL plug-ins for IIS, Apache, cPanel or Parallels Plesk to redeem the voucher. Redemption of the voucher means the plug-in will transparently create the CSR, validate the domain control, install the issued certificate and bind it to the appropriate website. The Admin will have a fully valid, trusted and active SSL Certificate operational on the site in 30-45 seconds. OneClickSSL will dramatically reduce the support overhead of managing SSL for customers, or even for enterprise servers. The below screenshot from cPanel shows how simple the user experience becomes when redeeming a OneClickSSL voucher:



LOOKING AT THE PROCESS IN DETAIL

The technology behind OneClickSSL is based on multi-factor authentication techniques.

For example, US Federal regulators consistently recognize three authentication factors:

"Existing authentication methodologies involve three basic "factors":

- **Something the user knows (e.g. password, PIN)**
- **Something the user has (e.g., ATM card, smart card)**
- **Something the user is (e.g., biometric characteristic, such as a fingerprint)**

Authentication methods that depend on more than one factor are more difficult to compromise than single-factor methods." (FFIEC).

Multi-factor Authentication with OneClickSSL

"One problem with multi-factor authentication generally is the lack of understanding of what constitutes "true" multi-factor authentication. Supplying a user name ("something the user knows") and password ("something the user knows") is single factor authentication, despite the use of multiple pieces of distinct information. Supplying

additional information in the form of answers to challenge questions (more of "something the user knows") is still single-factor authentication". (Wikipedia)

An example of true multi-factor authentication is requiring that the user insert a Smart Card into a Smart Card Reader (something the user has) and enter in a Password (something the user knows). Requiring a valid fingerprint via biometric fingerprint reader would add a third factor.

With OneClickSSL we can amend the example slightly as follows:

- **Something the user knows (Voucher)**
- **Something the user has (A 2048 bit RSA private and public key pair)**
- **Something the user is (A domain that is registered on the DNS system and verifiable)**

If the user is able to provide positive affirmation of the control of a domain by installing a test certificate and successfully answering a https based TLS challenge/response on their chosen domain, they may legitimately be given a publically trusted certificate for the same domain (using the same key pair they have already shown possession of).

IIS 6, 7 and 7.5 oneclickssl.exe

To provide maximum flexibility for administrators of IIS web servers, GlobalSign has created a Command Line Input (CLI) tool. Running the tool in debug mode highlights the process in more details and the commentary along the side provides clarification of key points.

```
C:\Windows\system32\oneclickssl DVY4TN1UVD0NL4F6 oneclickssl.globalsign.com -
natip 192.168.2.3 -debug
```

```
GlobalSign OneClickSSL(tm) Installer v1.0.1 (c)GMO GlobalSign, 2011
=====
```

Use this application to redeem OneClickSSL Vouchers and automatically activate SSL security and the "secure padlock" for your website.

OneClickSSL secure site activation in process.

Do not close or navigate away from this page until completed...

```
Determining Windows Version
SUCCEEDED - Running on Windows 2008/IIS7 or IIS 7.5
No external IP address was entered so looking up the domain via a DNS
search...
SUCCEEDED - We found the Domain's IP address as : 80.46.115.103
The Internal Network Address Translation IP address used is : 192.168.2.3
Connecting to GlobalSign's 'PRODUCTION' webservice URL for OneClickSSL
Checking IIS for the 'oneclickssl.globalsign.com' website
SUCCEEDED - IIS website found and there is no existing certificate or
binding
for this IP and port combination
```

Sending Voucher & Domain details to the GlobalSign OneClickSSL service...

```
Receiving Voucher validation check response including a Phishing Check &
domain
Keyword analysis...
NOTE : This OrderID for the 'TEST' certificate will be useful if you need
to
talk to our support team :-CEVT1102110755
'GlobalSign Root CAT' root certificate must be added to the Certificate Store
Generating Root Certificate file...
Registering Root Certificate...
SUCCEEDED - The Root Certificate was successfully added to the Root Store.
Checking for existing matching requests...
Processing new CSR
Generating new certificate request...
SUCCEEDED - CSR generated is as follows...
```

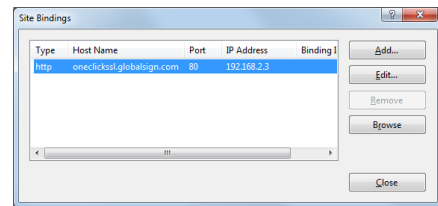
```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIID4jCCAsocAQAwMjELMAkGALUEBhMCR0IxIzAhBgNVBAMGM9uZWNsaWNrc3Ns
Lmdsb2JhbHNPZ24uY29tMlIIBjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAK
COBQWR2ktd3d6xYAiEfB9F+hJRJ7aBKtQbWwIUaK48qoH6HrPBEunwOspyyvi
4Z6YigkTISTel71YBKHueRNmqP6JUGUXEmnTs3X7Lsx0On4kI7mG2KzkL4xnOC/
.....
Truncated for this white paper
.....
4x01gv38edJLSITo9P3RmXOEqlc7kpVak9F1UW616tIHqB7dGdGtEnhb/ZFIVatP
yeTWvfUvy2UVt5cP6/VTYJkEIV3+UyBUALtj5toRBIT/4Ri3mJyJunv+f01qOT9U
A9OpMlMAcwn/UIDwrtLfmPpSyYQHWDulZ5FWNp+fhyPdRiXdlkQ1Oe2AgYteDb6W
hsvtt6vB4Ju1xdY4K3WI/STQnYXjfwMwhcwVWnCN/E+cZtFYvM=
-----END NEW CERTIFICATE REQUEST-----
```

```
Analysing and processing new CSR request...
SUCCEEDED - Found CSR thumbprint :-
'669702E7322EC1CAB706D9ABAF202DF692952E2B'
Sending TEST certificate request...
Receiving TEST certificate response...
NOTE : This OrderID for the 'PRODUCTION' certificate will be useful if you
need to talk to our support team :-CEVT1102110756
The following certificate will be installed...
```

```
-----BEGIN PKCS7-----
MIINAgIJKoZThvcNAQcCoIIM8zCCD08CAQExADALBgkqhkiG9w0BBwGgggzXMIIE
4zCCA8ugAwIBAgILAQAAAAABLhSImD4wDQYJKoZIhvcNAQEFBQAwbDEKMCIGALUE
CxMbT3JnYW5pemF0aW9uIFZhbG1kYXRpb24gQ0FUMRMwEQYDVQQKEwpHbG9iYXN0
aWduMS8wLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEw
IENBVDAeFw0xMTAyMTEyMTEyMTEyMTEyMTEyMTEyMTEyMTEyMTEyMTEyMTEyMTEy
c2lnbi5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQ9rgzaUfs6
SgpflBIAchVlryD/Z0sAI5GDRnCuQRkRtXsTWE090BGw8OXv27ElnvXAXa3TB113
.....
```

The command line tool for IIS is run with the following parameters in debug mode to deliver a DomainSSL Certificate:

Voucher	DVY4TN1UVD0NL4F6
Domain	oneclickssl.globalsign.com
NATIP	192.168.2.3



The domain on IIS is verified as is the setup of IIS. The validity of the voucher is checked as well as the name of the domain. DomainSSL Certificates, as with all SSL Certificates from GlobalSign can only be issued to websites that have not been blacklisted for phishing. Keyword analysis was performed at the point of issuance of the voucher but will also be checked here too.

A successful check of the voucher allows an OrderID for the 'Test' certificate to be captured CEVT1102110755.

The CSR is automatically generated within IIS. Only the CN (Common name) of the domain is necessary for inclusion within the CSR. GlobalSign adds any necessary verified data to the final certificate later on. Data will have been pre-verified during the purchasing process to obtain the voucher.

The CSR and order number are sent to GlobalSign. The response is another OrderID for the final 'Production Certificate' and a PKCS#7 test certificate CEVT1102110756.

```

Truncated for this white paper
.....
i0jZnyZP6CBCNnugllh5Chm93CMLjugdh3tKRwQ/Zu9ruVdauTEQXGovrZHpP4O
3wMxg/2pr3mSyPliC51flpOadoHmNecVP53tcTFK5Z8Qne4T3U2IK/4/19Z40XIg
p79sAQHGPEvNwF30G7IUTBjFab88CAWF9D+/EHMwTsVM9gzmQ/0G2yjk1PeUoKpa
eqeesTNGiG9cdkTT40u/+DKKXqcxAA==
-----END PKCS7-----

Installing Certificate...
Validating Certificate installation
SUCCEDED - Found 'F38B48204C8A084C5381A08784B2F5E059BBFE87'
Assigning test certificate to the website...
Looking for existing IIS binding
Removing existing IIS binding
Adding new IIS binding
Checking for existing matching requests...
Processing new CSR
Generating new certificate request...
SUCCEDED - CSR generated is as follows...

-----BEGIN NEW CERTIFICATE REQUEST-----
MIID4jCCAsCAQAwMjELMAkGA1UEBhMCROIxIzAhBgNVBAMGM9uZWNsaW93N3Ns
Lmdsb2JhbHhpb2Z24uY292tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
kCOBQwR2kt3d36xYAiEfB9F+hJRJ7aBktQbWwIUaKnl48qoH6HrPBEunwOspyyvi
4Z6YigkTISTe171YBKHueRNmqP6UJGUXEmnTs3X7LsX0On4kI7mG2Kzk8L4xnOC/
1SimPsiXaQ4USCLAsEk3XHNjveYvJrONuZ6n4cV/ojokVZ5TNZakFiCkr37hZ5nh
.....
Truncated for this white paper
.....
BHCwDQYJKoZIhvcNAQEFBQADggEBABXEFRobmhIzbyzsaMZB5wrotOyWlR6Sym/d
iy38wryBoLc3LXpoYMLLd4jZuH2Md/spIDOrCmCxbWRJF5nco41NEs5domDrxWcu
4x01gv38edJLSITo9P3RmXOEQLo7kpVAK9F1UW616tIHQb7dGdGtEnhb/ZFIvatP
yeTWvFUVy2UVt5cP6/VTYJkEIV3+UyBUALTj5toRBIT/4Ri3mJyJunv+f01qOT9U
A9OpMLMAcWn/UIDwrtLfmMPSyYQHWDu1Z5FWNp+fhyPdRlxDkQ1Oe2AgYteb6w
hsvtt6vB4JujlxdY4K3WI/STQnYXjfwMwhcwVWnCN/E+cZtFvM=
-----END NEW CERTIFICATE REQUEST-----

Analysing and processing new CSR request...
SUCCEDED - Found CSR thumbprint :-
'175F194BEF28D60BA898E9A16F44FA427D9C7CB2'
Sending PRODUCTION certificate request...
Performing domain verification check and Enrolling for an SSL certificate
-----
Receiving PRODUCTION certificate response
SUCCEDED - Certificate serial number is :-010000000012e1488d2fb
The following certificate will be installed...

-----BEGIN PKCS7-----
MIINiWYJKoZIhvcNAQcCoIINFDCDRACAQExADALBgkqhkiG9w0BBwGgggz4MIIF
CTCCA/ggAwIBAgILAQAAAAABLhSI0vswDQYJKoZIhvcNAQEFBQAwTElMAkGA1UE
BhMCUKXHTAaBgNVBAsTFERvbWVpbiBwYXNjaW9uIENBMkRkFwYDQKQkExBh
.....
Truncated for this white paper
.....
GkUN18qJUC99BM00qP/8/UswDQYJKoZIhvcNAQEFBQADggEBANZ53xPdtCNv+y6
or40xSgytXz8bJwsK70Jn10/a16qEui25Qijs8o9YU3TRgmzPsOg42NVG/K67605
4UO5OKFmL4omO+ggUf5xgr9OM3EC3BRLJeYBN/DX5TVFckUQzEXXvkFQ3/VTDs
ho//De8suWNG9qr837xp/S4SSGSa4JXwpu8pJwGxFbUMHaX+aSxpJHges6cccWLu
ysiXrBddisL4R4ZuKsRWMXQZ4mFK/lsp11GnQyqguSZUdlwt9tWPHWkauFclvb+
Pd5BzAeuY1K/U1P0K+nH/bb3gl+F0kEY24GzBBzFH6SAbxUgyd4MiAodimZV4vxI
ySkmaeAxA==
-----END PKCS7-----

Installing Certificate...
Validating Certificate installation
SUCCEDED - Found '7D7A26AFFD150E27FE79FDED7E2DF25CFE7499F9'
Assigning PRODUCTION certificate to the website
Looking for existing IIS binding
Removing existing IIS binding
Adding new IIS binding
Cleaning up the test certificate...
Removing certificate with
Thumbprint: 'F38B48204C8A084C5381A08784B2F5E059BBFE87'

OneClickSSL secure site setup successful!
-----
Press any key to continue...

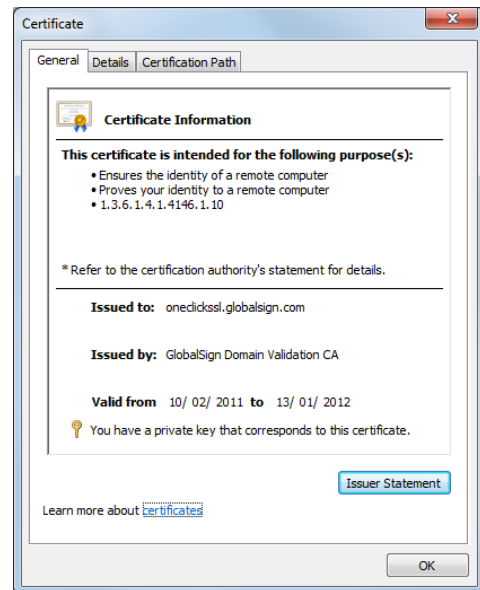
```

The test certificate is captured and installed into IIS.

A new CSR is created (Using the same keys and same CN) and sent back to GlobalSign with the 'production' OrderID.

There is no risk for the two OrderID's to be incremental as the two CSRs MUST use the same keys and have the same Common name.

The production certificate is received and installed including the intermediate issuing CA.



Test certificates are purged from IIS and the program finishes.

BENEFITS OF PARTNERING WITH GLOBALSIGN

Hosting Companies

Hosting companies can use the GlobalSign Certificate Center (GCC) or XML API to apply for individual Secure Site vouchers to be redeemed using any of the OneClickSSL client plug-ins. Alternatively single “supervouchers” can be issued that can be reused across the entire hosting customer base, allowing hosting companies to easily mass provision SSL. Hosting companies can restrict the IP range to which vouchers may be redeemed, ensuring they remain in full control of the OneClickSSL plug-in usage on their networks and to restrict redemption of vouchers to those they manage/sell. OneClickSSL ensures that hosting companies have unlimited business potential and flexible models for deploying SSL to their customer base. Never before has SSL been so controllable on a hosted network.

Generate a new revenue stream / augment existing revenue stream

The use of SSL is now a key aspect of online security and is a requirement for any organization that has an online presence (to protect customers against phishing attacks, credit card fraud and identity theft, whilst protecting the organization's brand and reputation against fraudulent websites). So why not take advantage of this opportunity to not only sell SSL Certificates, but to provision secure sites across your network with zero support overheads and a dramatically improved customer experience?

- **Offer Secure Site Vouchers and prevent clients from purchasing their SSL elsewhere**

Being successful in a highly competitive market is extremely difficult, so differentiate from competitors with OneClickSSL. Activation of “secure sites” can be offered as part of an existing package, producing a comprehensive hosting product portfolio. GlobalSign's SSL technology is a superior product in the market place by means of deployment, feature set, compatibility and account management/technical support. As well as expanding the organization's product portfolio, the organization will be able to offer the most secure and advanced SSL products available.

SSL Certificate Features:

- **Guaranteed best security practices via OneClickSSL – key size and strength and crypto algorithms are all dictated and managed by the plug-ins, not the user**
- **Website security that's trusted by all browsers, applications and mobile devices**
- **Unlimited server licensing – a single certificate can secure an unlimited number of physical servers**
- **Strong security – SGC included in all GlobalSign certificates free of charge**
- **Issued from a 2048 bit root (globally embedded since 1998)**
- **Secures both www and non-www with single certificate**
- **Warranty**
- **Clickable Site Seal**
- **Worry free refund policy**

Reduce your Support Costs

Many hosting companies lose any margin they may have made with SSL when they need to be directly involved with reissuing certificates, or answering questions on lost keys, or having to generate the CSR on behalf of the customer. OneClickSSL allows your support staff to focus their time and efforts on the bigger issues, giving them opportunity to provide even better customer support. OneClickSSL revolutionises how hosting companies offer and support SSL Certificates across their network and opens the market for hosting companies of all sizes to offer “secure sites” to the masses, without the fear of increased support overheads.

PARTNER PROGRAM LEVELS

GlobalSign offers 4 levels of Partnership – Authorized, Silver, Gold and Platinum.

Authorized Partners receive instant discounts, a reseller partner portal (GlobalSign Certificate Center), canned sales and marketing resources and instant access to technical support.

Silver, Gold and Platinum Partners receive accelerated discounts, access to the advanced APIs, control panel plug-ins, dedicated marketing assistance, varying levels of co-marketing/co-branding opportunities and feature prioritization.



WHY PARTNER WITH GLOBALSIGN?

With fantastic margins and increased revenue potential, this is a simple, but sophisticated reseller program enabling you to generate new revenue streams, expand your product portfolio and provide the best SSL and Malware Monitoring there is available. The program is built around the needs of hosting companies, fulfilling both technical and marketing requirements:



The program has an extremely fast return on investment with the option of no commitment. It also involves minimal time, effort and resources. But don't just take our word for it, ask any of our thousands of hosting partners...

"We chose GlobalSign based on reliability, cost and overall ROI. Our customers have increasing security concerns which prompted us to find a provider who could offer the most reliable and cost effective SSL security solution."
Travis Stoliker, Marketing Director



"It is vitally important to us that we partner with the most credible and forward thinking vendors for every third party service we offer. Since the start of our relationship we've been able to pass on the value of the GlobalSign brand as well as the strong security its products offer. Our partnership has many co-marketing initiatives and development plans in place, with on-going industry leading improvements in certificate issuance workflows, as well as continued education to our customers about online security threats - leading to a customer experience both our companies can be proud of."
Thomas Vollrath, CEO, Webfusion



INQUIRE ABOUT ONECLICKSSL & THE PARTNER PROGRAM

To join now, or for further information about becoming a GlobalSign SSL Partner and OneClickSSL visit our website at www.globalsign.com/partners.

ABOUT GLOBALSIGN

GlobalSign was one of the first Certification Authorities and has been providing digital credentialing services since 1996. It operates multi-lingual sales and technical support offices in London, Brussels, Boston, Tokyo and Shanghai.

GlobalSign has a rich history of investors, including ING Bank and Vodafone. Now part of a GMO Internet Inc group company - a public company quoted on the prestigious Tokyo Stock Exchange (TSE: 9449) whose shareholders include Yahoo! Japan, Morgan Stanley and Credit Suisse First Boston.

As a leader in public trust services, GlobalSign Certificates are trusted by all popular Browsers, Operating Systems, Devices and Applications and include SSL, Code Signing, Adobe CDS Digital IDs, Email & Authentication, Enterprise Digital Solutions, internal PKI & Microsoft Certificate Service root signing. It's trusted root CA Certificates are recognized by all operating systems, all major web browsers, web servers, email clients and Internet applications; as well as all mobile devices.

Accredited to the highest standards

As a WebTrust accredited public Certificate Authority, our core solutions allow our thousands of enterprise customers to conduct secure online transactions and data submission, and provide tamper-proof distributable code as well as being able to bind identities to Digital Certificates for S/MIME email encryption and remote two factor authentication, such as SSL VPNs.

For more information about the GlobalSign solutions, please contact us:

Singapore

Tel: +65 3158-0346
sales-apac@globalsign.com
www.globalsign.com.sg

Australia

Tel: +61 3-9988-3988
sales-apac@globalsign.com
www.globalsign.com.au

Hong Kong

Tel: +852 5808-1867
sales-apac@globalsign.com
hk.globalsign.com