WHITE PAPER

Why a New Business Model is Needed for SSL Certificates

An Osterman Research White Paper

Published June 2013

SPONSORED BY

Osterman Research, Inc.
P.O. Box 1058 • Black Diamond, Washington • 98010-1058 • USA
Tel: +1 253 630 5839 • Fax: +1 253 458 0934 • info@ostermanresearch.com
www.ostermanresearch.com • twitter.com/mosterman

EXECUTIVE SUMMARY

The de facto Internet communication security protocol in use today is Secure Sockets Layer (SSL), used most commonly for browser-to-Web server communications, but increasingly for connections between applications when transferring critical business content. SSL has been successful because of its ease of use and the fact that certificates can be procured with relative ease. SSL has gained further prominence during the past few years because of the rapid uptake of the cloud and the growing number of transactions on the Web.

THREE KEY TAKEAWAYS

However, there are three fundamental problems with the current state of SSL:

- **SSL is underutilized as a way to increase security and business**
  There are varying levels of security that can be found in an SSL certificate, ranging from self-signed (least trusted and secure) through to Extended Validation (EV) certificates (publicly-rooted and highly trusted). The benefits of using EV certificates are two-fold: 1) the visual representation in the browser in which EV is being used – the browser address bar turns green – gives end users a clear understanding that they are on a trusted site, which can result in a significant sales uplift; and 2) the vetting process used to issue EV certificates is extremely rigorous and as such, delivers a more trusted and secure certificate. The challenge is that even though EV certificates offer the highest level of security, they are the least commonly used because of their high cost and the greater difficulty associated with acquiring them.

- **There have been numerous security breaches**
  If there was a "Year of the Data Breach", then the past year certainly was it. Numerous issuers of SSL certificates – Certificate Authorities, or CAs – were compromised and bogus certificates were issued, creating significant data breaches with disastrous consequences in some cases. Contributing to the problem is that most CAs extend complete trust for certificate issuance to Local Registration Authorities, affiliates or resellers (referred to in this white paper as CA affiliates) in order to increase revenue or market share. This extension of trust enables potentially risky organizations with less-robust processes to issue certificates that may use bogus information without the root CA ever knowing it.

- **The current certificate acquisition model is fueling the problem**
  In an ideal world, all SSL certificates for both internal and external Web servers would be at a minimum publicly rooted, but even better EV certificates because they require the most rigorous vetting process for applicants and they offer the highest level of assurance to users that their transactions are safe (e.g., a green bar in the URL space of Web browsers). However, the per-unit pricing model for all types of SSL certificates, including the more expensive EV certificates, combined with the high cost of tracking and managing them internally, makes this ideal scenario impractical and unaffordable for many organizations. Combined with the need to issue and manage more and more SSL certificates for application-to-application security, it's clear that the per-unit approach to SSL certificate acquisition needs to change.

What is needed, therefore, is a) a less expensive way to implement SSL certificates, b) a reliable way to acquire them from a trusted source, and c) a pricing model that will not force decision makers into a tradeoff between the cost of more secure certificates and the security of their infrastructure.

ABOUT THIS WHITE PAPER

This white paper discusses the current problems with SSL, provides an overview of the technology, and offers suggestions on ways to improve the acquisition and management of SSL certificates. The paper also provides a brief overview of Trend Micro and its SSL-related offerings.

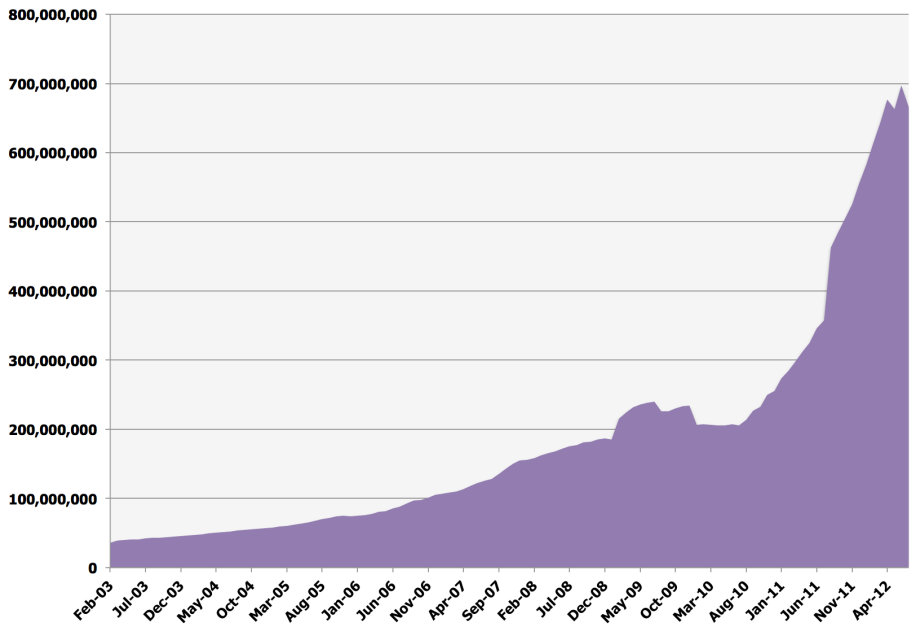
In an ideal world, all SSL certificates would be EV certificates. However, the high cost of EV certificates, the per-unit pricing model for acquiring them, and the high of tracking and managing them internally makes this ideal scenario impractical and unaffordable for many organizations.

APPLICATIONS AND E-COMMERCE ARE AT RISK

THE NUMBER OF WEB SERVERS IS EXPLODING

Supporting the growth of cloud computing and the rapidly expanding number of applications available via a cloud model is a rapidly increasing number of Web servers. A review of Netcraft's statistics, for example, shows the meteoric growth of Web Servers to nearly 700 million Web servers worldwide[i]. Moreover, the number of worldwide Internet users increased 528% between 2000 and 2011[ii].

Total Web Sites Across All Domains
February 2003 to July 2012



Source: Netcraft, July 2012

SERVICES ARE INCREASINGLY DELIVERED USING A CLOUD MODEL

The sheer volume of services that are delivered using a cloud model is increasing at a rapid pace. For example:

- Morgan Stanley anticipates that public cloud delivery of various workloads will increase at a 50% compound annual growth rate between 2010 and 2013, while private cloud/virtualized workloads in on-premise environments will increase from 32% of workloads to 52% during the same period[iii].
- Forrester estimates that the cloud computing market will grow from $41 billion in 2011 to $241 billion by 2020[iv].
- Gartner has estimated that the cloud computing market will increase from $68.3 billion in 2010 to $148.8 billion by 2014[v].
- Underscoring the growing importance of cloud computing is data from Wanted Analytics that shows the number of cloud computing jobs advertised online in April 2012 exceeded 12,000 – representing an increase of 49% compared to April 2011 and 275% more than in April 2010[vi].

One of the most serious security issues during 2011 was the breach of many certificate authority (CA) infrastructures.

- Traditional e-commerce, one of the older cloud services, continues to grow at a rapid pace. For example, Amazon.com's sales for the last three months of 2011 were $17.43 billion, up 35% compared to a year earlier.

THE RISKS ARE ALSO INCREASING

At the same time, the risks associated with managing applications in the cloud are increasing as Web servers are increasingly vulnerable to attacks of various types. For example:

- **Advanced persistent threats (APTs)** are a particularly serious problem from a Web server security perspective because these tend to be coordinated attacks, sometimes from well-funded and dedicated sources, as opposed to more opportunistic attacks. An APT can use a variety of methods to penetrate defenses, including malware delivered via the Web or email, infected flash drives, Wi-Fi access or any of a variety of other methods. While not always the case, an APT is often the result of state-sponsored efforts.

- **Malware** is also a very serious threat for Web servers because of the varied abilities of worms, spyware, adware, Trojan horses, rootkits and other programs to disable servers, steal data, raid financial accounts and create other problems.

- **Man-in-the-middle attacks** are another serious problem because of the threat they pose to authentication capabilities and the trust that can be lost as a result.

- **Direct hacker attacks**, one of the more popular of which is a denial-of-service (DoS) attack, are often relatively unsophisticated efforts to flood a particular Web server or set of servers with traffic until they crash. These types of attacks have been used to bring down numerous Web sites worldwide, including high profile targets like the Web sites of the FBI and the Recording Industry Association of America.

MANY CAs HAVE BEEN COMPROMISED

One of the most serious security issues today is the breach of many certificate authority (CA) infrastructures. For example:

- In November 2011, Malaysian intermediate CA Digicert, an Entrust affiliate (not connected to Utah-based DigiCert), had trust in all of its certificates revoked by Microsoft and Mozilla after the CA had issued 22 certificates with weak 512-bit keys, among other problems[vii].

- In March 2011, Comodo was the target of an Iranian hacker who forged bogus certificates for Google's email services[viii].

- In June 2011, StartSSL stopped issuing certificates after discovery of a security breach[ix].

- In August 2011, an intrusion into DigiNotar's CA infrastructure resulted in the issuance of bogus public key certificate requests[x] and the ultimate bankruptcy of the company.

- In September 2011, Globalsign discovered a breach in a Web server hosting its Web site[xi].

- In December 2011, the Dutch company Gemnet was compromised and KPN, its CA division, suspended access to its Web site as a precaution[xii]. This followed a November 2011 incident in which KPN stopped issuing certificates after discovering a DDoS tool in its Web infrastructure[xiii].

All told, at least a dozen major CA breaches occurred in a single 12-month period.

CA breaches result in a loss of trust. For example, in the immediate aftermath of a CA breach, the affected CA will lose the trust of at least some of its customers – if not most of them – and it will lose business during the investigation phase when certificates are not being issued.

USE OF THIRD PARTIES CAN INCREASE RISK

Many CAs use affiliates to issue SSL certificates, creating another potential source of CA breaches. For example, recently one of Comodo's affiliates issued an SSL certificate to a party that it did not verify[xiv]. In another case, the founder of StartCom conducted an experiment to demonstrate the lack of security precautions that are exercised by some CAs. Using a Comodo affiliate, he created a certificate for mozilla.com – a domain he obviously did not own – and received a legitimate certificate within five minutes. The affiliates did not conduct any sort of verification checks and asked no questions before issuing the certificate[xv].

It is important to note that we are not impugning the reputation of all certificate affiliates – for example, some CA affiliates are used for the sales process, but the vetting of applicants and delivery of certificates is performed by the CAs themselves. However, in many cases the use of CA affiliates does introduce a potential source of security breaches because of the lack of control that some CAs may exercise over their affiliate communities. For example, if a CA permits an affiliate to issue certificates on its behalf and does not conduct frequent audits of these affiliates, it leaves itself open to substantial risk.

THE CONSEQUENCES OF REDUCED ONLINE SECURITY ARE VERY SERIOUS

If CAs are breached, or if the security of Web servers cannot be maintained at the highest possible level, there are several serious consequences that can result. For example, in the case of a DigiNotar incident in which the company issued a fraudulent certificate for Google[xvi], the Iranian government was potentially able to spy on some of its citizens – possibly with life-threatening results. A breach that impacts a bank could permit a criminal organization to intercept customers' credit card numbers or bank login information and steal tens or hundreds of thousands of dollars from unsuspecting customers. Similarly, a CA breach could result in a company losing its intellectual property and with it the loss of millions of dollars of unrealized future revenue.

More fundamentally, CA breaches result in a loss of trust. For example, in the immediate aftermath of a CA breach, the affected CA will lose the trust of at least some of its customers – if not most of them – and it will lose business during the investigation phase when certificates are not being issued. Longer term, however, CA breaches also impact the perceived integrity of all certificate-issuing authorities, as well as their customers.

The critical question for many users is a simple one: if they cannot trust a CA, can they trust the company that depends on that CA? If the answer to that question is *No*, then e-commerce and other Web-based activities will slow or at least continue at a slower pace.

Organizations need to exercise great care during the certificate registration process, ideally delegating the process only to highly trusted third parties to ensure that only legitimate parties are receiving certificates.

HOW TO PROTECT AGAINST RISKS

Clearly, security must be improved in order to minimize the types of risks discussed above. Toward this end, we recommend that organizations implement two critical best practices:

- **Improve the certificate registration process**
  Organizations need to exercise great care during the certificate registration process, ideally delegating the process only to highly trusted third parties to ensure that only legitimate parties are receiving certificates. A failure to ensure the integrity of the certificate registration process can lead to the types of breaches noted above and, more strategically, to a loss of trust among customers and business partners. While the breaches themselves are bad enough, the loss of trust can lead to far-reaching and significant impacts on revenues and long-term business opportunities.

- **Differentiate the browser experience**
  Another critical best practice is to ensure that users experience the most secure browser experience possible – namely, through the use of Extended Validation (EV) certificates. Where appropriate, use Organization Validation (OV) certificates (ex: machine-to-machine transactions) to protect online transactions. The use of less secure Domain Validation (DV) should be avoided completely.

  EV certificates provide the most secure form of SSL validation because the organization requesting it is more carefully vetted to ensure its bona fides. An organization requesting an EV certificate must provide multiple pieces of information about itself, as well as about the organizational contact(s) listed in the enrollment application. The CA/Browser Forum has issued specific guidelines[xvii] about how EV certificates are issued and managed. For end users, the most obvious benefit of an EV certificate is that a Web browser will display a green bar in the URL space, clearly indicating that the site can almost certainly be trusted.

  By contrast, DV certificate requestors are vetted only by checking their right to use a particular domain name using an email challenge, but no background check on the applicant is conducted. The advantage of a DV certificate is that it can be issued very quickly, but the potential for issuing a certificate to a bogus entity is relatively high. An OV certificate, by contrast, is more secure because the CA will investigate the existence of the requesting organization and also determine whether or not the applicant has the right to use a particular domain name. Issuance of OV certificates is typically slower – usually requiring days instead of minutes as with DV certificates – but the security of the issued certificates is somewhat greater and a select few CAs are able to instantly delivery OV certificates through automated processes.

The bottom line is that SSL and properly granted certificates are essential to protect online application access, the integrity of transactions, and the overall level of trust between customers/users and organizations that rely on Web-based services. However, because not all certificates provide the same level of integrity, their use must be matched to the sensitivity of the data being accessed, as well as ensuring customer trust. Ultimately, the only way to achieve this in the Web browser is through EV certificates.

IMPROVED SSL SECURITY CAN RESULT IN MORE REVENUES

Not only do higher-level certificates (EV) provide more security for consumers of Web services and greater trust in the organizations that use them, higher-level certificates result in increased revenues. The Online Trust Alliance reports Web sites using EV certificates experienced increased buyer-clickthrough rates of 10% or higher[xviii]. One company reported that after it had switched to the use of EV certificates, its customer conversion rate increased by 41% and its revenue per transaction increased by 58%[xix].

Clearly, there is a strong relationship between the type of SSL certificate used its effectiveness in driving new business to the organization using it.

The Online Trust Alliance reports that many Web sites using EV certificates are reporting increased buyer-clickthrough rates of 10% or higher.

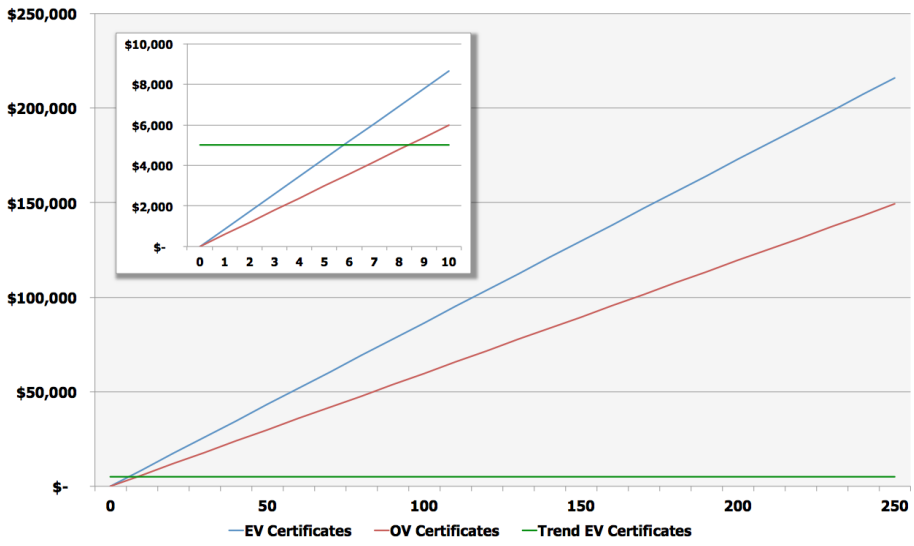
One company reported that after it had switched to the use of EV certificates, its customer conversion rate increased by 41% and its revenue per transaction increased by 58%.

THE NEED FOR A NEW BUSINESS AND PRICING MODEL

OUTDATED PRICING MODELS MAKE SSL EXPENSIVE

One of the major drawbacks of SSL certificates in general, and EV certificates in particular, is their high cost. For example, the price for a single-year EV certificate averages close to $1,000 and OV certificates start at over $300. To demonstrate how the cost of SSL certificates increases with volume, an average of leading SSL provider pricing is shown below for 1 to 250 certificates for both EV and OV. Also shown is Trend Micro's new flat rate pricing across the same number of certificates, highlighting the difference in pricing approaches and overall cost.

Traditional vs. Trend Micro SSL Certificate Pricing



The price differential for EV certificates is substantial compared to less secure certificates: for example, DV certificates can range from $50 to $269 from leading SSL certificate vendors. As a result, the much lower cost of DV and OV certificates relative to their EV counterparts prompts many organizations not to deploy EV certificates simply because they are too expensive. This reduces the overall security of Web-based transactions and, by extension, reduces the trust that individuals and businesses have when doing e-commerce via the Web. Moreover, as noted earlier, because the use of EV certificates can lead to greater revenue opportunities, not using EV has a negative impact on overall revenue growth.

THE CURRENT PURCHASE MODEL ALSO SLOWS DEPLOYMENT

Another impediment to the use of EV certificates, and the broader use of publicly rooted certificates for external and internal applications in general, is the current pricing model that charges customers on per-unit basis. Not only does this require justification of each new certificate purchase in some cases, it also motivates cost-conscious decision makers to purchase less secure DV and OV certificates when EV certificates will provide the appropriate level of security. These tradeoffs may provide some short-term cost savings, but can create dramatic impacts down the road in the event of security breaches, lost revenue opportunities and the like. Plus, in many organizations the cost of SSL certificates is borne by an IT or security function that may realize only faster depletion of its budget when purchasing EV certificates and not the advantage of greater revenue that benefits the overall organization.

Another impediment to the use of EV certificates, and the broader use of publicly rooted certificates for external and internal applications in general, is the current pricing model that charges customers on per-unit basis.

The problem is particularly serious for organizations that need to purchase SSL certificates only for temporary spikes in demand, such as retailers who anticipate a large number of sales during the Christmas season. It also increases the cost of moving applications from testing to external-facing status, as most organizations will use self-signed certificates for development and testing, forcing a significant re-test effort when going external and using a publicly-rooted certificate. This both slows deployment and increases internal development costs all based on not having to purchase too many publicly rooted SSL certificates.

It is also important to note that the tracking requirements for multiple, individual purchases of certificates is a cumbersome process that leads to significant internal management costs and unnecessary procurement delays.

CERTIFICATE COST AND MANAGEMENT SHOULD BE VIEWED HOLISTICALLY

As a result of the issues discussed above, Osterman Research recommends that decision makers seriously consider doing four things:

1. View certificate cost and management in a more holistic fashion, considering them as critical components of an overall security spend by an organization.

2. Business stakeholders – not just security – should be involved in the security management process, since EV certificates lead to more revenue than use of their DV and OV counterparts, which benefits the overall organization. Certificate management and purchase decisions should be viewed not only defensively, but also as a means of boosting customer purchases, improving customer retention and increasing the average amount of revenue per customer.

3. Focus on purchasing the most secure certificates at the lowest possible cost, leveraging them for both external and internal applications where appropriate.

4. Purchase certificates directly from a CA (not an affiliate) to reduce risk and the potential for data breaches.

ABOUT THE TREND MICRO SSL SERVICE

The Trend Micro SSL service is built on an innovative business model that offers unlimited OV and EV SSL certificates using a flat-rate pricing model. This enables organizations with the ability to instantly deploy widely trusted certificates with the highest security possible without bearing the high cost and effort levels required by other CAs. Trend Micro customers receive all of this for one low, flat rate that will save significant amounts of acquisition and management costs, and naturally fits the dynamic nature of the cloud.

Moreover, to preserve the security of the issuance process, the Trend Micro service exclusively delivers SSL certificates directly to its customers and not through affiliates. This removes the risk associated with other vendors' use of affiliates, subcontractors or resellers to generate and issue certificates that has been the focus of attacks in the past. Instead, Trend Micro leverages its traditional selling channel to manage the sales process, but will reserve the vetting and direct delivery of certificates to end customers only for Trend Micro.

TREND MICRO: A DIFFERENT APPROACH TO SSL

As a global leader in security, Trend Micro saw customers struggling with the reality of today's SSL *business* and the needs of tomorrow around cloud security. It became clear that a new approach to the SSL business was required; one that could provide organizations with the means to secure all communications in a significantly more trusted and more cost-effective way. Given that most organizations are in the growth phase of embracing the power of cloud computing and will continue to need SSL

Another impediment to the use of EV certificates, and to a lesser extent the use of certificates in general, is the current pricing model that charges customers on per-unit basis.

security for traditionally deployed applications, Trend Micro believes SSL is a natural offering from a world leader in security.

Trend Micro's SSL service is built on an experienced team of SSL experts - the same team that grew GeoTrust into a leading global brand for SSL certificates. Members of this widely respected team were also founding members of the CA/Browser forum, the key industry body for SSL, and continue to be active in the organization.

Trend Micro delivers a new SSL business model with SSL certificates that are trusted across over 99% of browsers and backed by the support of proven SSL security experts.

Part of its Web App Security solution, Trend Micro's service marks a new way of delivering SSL capability, where trust is not subcontracted to third parties for certificate issuance and a per-certificate model that forces organizations to compromise on trust is a thing of the past.

The Trend Micro service marks a new way of delivering SSL capability, where trust is not subcontracted to third parties for certificate issuance and a per-certificate model that forces organizations to compromise on trust is a thing of the past.

---

[i] http://news.netcraft.com/

[ii] http://www.internetworldstats.com/stats.htm

[iii] http://www.morganstanley.com/views/perspectives/cloud_computing.pdf

[iv] http://blogs.wsj.com/digits/2011/04/21/more-predictions-on-the-huge-growth-of-cloud-computing/

[v] http://www.siia.net/index.php?option=com_content&view=article&id=797:cloud-computing-benefits-economic-growth&catid=163:public-policy-articles

[vi] http://www.wantedanalytics.com/press/2012/05/23/the-sky-is-the-limit-for-cloud-computing-hiring/

[vii] http://www.pcworld.com/businesscenter/article/243170/mozilla_microsoft_withdraw_trust_in_malaysian_intermediate_ca.html

[viii] http://pastebin.com/74KXCaEZ

[ix] http://news.netcraft.com/archives/2011/06/22/startssl-suspends-services-after-security-breach.html

[x] http://www.vasco.com/company/about_vasco/press_room/news_archive/2011/news_diginotar_reports_security_incident.aspx

[xi] https://www.globalsign.com/company/press/090611-security-response.html

[xii] http://nakedsecurity.sophos.com/2011/12/08/second-dutch-security-firm-hacked-unsecured-phpmyadmin-implicated/

[xiii] http://hackmageddon.com/2011/12/10/another-certification-authority-breached-the-12th/

[xiv] http://news.netcraft.com/archives/2011/03/23/browsers-vulnerable-to-fraudulent-ssl-certificates.html

[xv] https://blog.startcom.org/?p=145

[xvi] http://googleonlinesecurity.blogspot.com/2011/08/update-on-attempted-man-in-middle.html

[xvii] http://www.cabforum.org/Guidelines_v1_3.pdf

[xviii] https://otalliance.org/resources/EV/index.html

[xix] http://blog.certs4less.com/case-study-ac-lens-gains-ground-on-the-competition-using-verisign-extended-validation-ssl/