100% Encrypted Web and the Use of Identity in SSL/TLS Certificates as a Proxy for User Safety

By Kirk Hall and Chris Bailey, Entrust Datacard

February 15, 2017

1. Executive Summary: SSL/TLS server certificates are essential to internet security for encryption and identity – of a domain and an organization.

Today the web is quickly moving toward 100% encryption because of several significant and systematic changes over the past few years that are driving even non-transaction oriented websites to quick and easy methods for receiving and managing SSL/TLS certificates. These changes have caused a rapid rise in SSL/TLS certificate use which is dramatically improving several aspects of Internet usage by protecting visitors to encrypted websites from Man-In-the-Middle (MITM) activities like spying and other attacks.

As with almost every major advance, there are also some unexpected negative outcomes. One fact is clear: fraudsters are moving to 100% encryption, using anonymous DV certificates almost exclusively. What’s more, current browser UI security indicators are conflicting, inconsistent, and constantly changing, leaving users confused. Google’s proposed new UI security indicators are a good start, but make no distinction between certificates that include confirmed identity information (in Organization Validated (OV) certificates) from certificates that do not (Domain Validated (DV) certificates), failing to utilize important information relating to user safety.

Accordingly, browsers should pivot to greater reliance on certificate identity information as a strong proxy for user safety, giving distinct and favorable UI security indicators for OV and EV certificates as safer for users than websites secured with only a DV certificate. This can be accomplished without changing the current browser UI security indicators, but instead by reassigning existing or proposed new security indicators based on the type of certificate securing a website.

Outline of White Paper:
1. Executive Summary
2. The History of Identity in Certificates and Browser UIs
3. Analysis of Recent Developments
4. Employing Identity Information as a Proxy for User Safety
5. A Proposal for Reassignment of Current Browser UI Indicators to Promote Identity and User Safety
6. Additional Industry Steps to Strengthen Certificates and User Safety
7. Five Principles of TLS Certificate Identity
The History of Identity in Certificates and Browser UIs:

(a) Early Years (1995-2001). When digital certificates were introduced in the 1990s, they were all one kind: essentially Organization Vetted (OV) certificates containing identity information in the O, L, S, and C fields (i.e., confirmed organization name and city, state, and country of location) in compliance with applicable RFCs. See RFC 1422¹ (1993) and RFC 3280 (2002).

Unfortunately, as explained in further detail below, encryption and the identity of a website were tied together from the start, which then leads to confused messaging that exists even today.² Also, there were no common procedures or minimum authentication requirements among CAs for OV certificates, CAs often failed to disclose much information about their authentication processes, and there were no WebTrust audit standards applicable to authentication, which meant the identity information in certificates was not equally reliable among CAs – some were highly reliable, while others were not.

The default state of the web, as with many other internet protocols, has been unencrypted communication, with security via the SSL protocol later added. Browsers at the time chose a binary UI hierarchy for displaying security states in their browser UIs. Users were trained to look for the padlock as a symbol of “safety” (both encryption and identity combined).

Unfortunately, none of the identity information inside the certificate was ever displayed to users in these early UIs, and users had to click on the padlock multiple times to see the website identity information (and the information was presented in a format that was not user-friendly).

<table>
<thead>
<tr>
<th></th>
<th>No certificate (http)</th>
<th>Normal state</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>OV Certificate with identity information - only OV certs in this period – (https)</td>
<td>Padlock</td>
</tr>
</tbody>
</table>

(b) Introduction of DV Certificates (2001). Not every website wanted to go to the trouble and expense of verifying its identity and buying OV certificates, especially when the only reward was the padlock icon but no display of that identity information. As a result, in 2001 CAs began offering Domain Validated (DV) certificates using automated, fast issuance, which lowered the price, made encryption more readily available, and helped increase the security of websites. However, website owner identity for a DV certificate is unknown and therefore unverified by anyone.

The browser UI hierarchy for displaying security states did not change to reflect the difference between these new DV certificates and the previously universal OV certificates – both received the identical padlock icon in the browser UI, and none of the OV identity information was ever displayed to users without clicking on the padlock multiple times.

¹ RFC 1422 (1993) states: 3.3.4 Subject Name - A certificate provides a representation of its subject's identity in the form of a Distinguished Name (DN). The fundamental binding ensured by the key management architecture is that between the public component and the user's identity in this form.

One possible reason the browser UIs never distinguished between DV and OV at that time is that OV vetting procedures still were not equivalent among CAs in the industry, and so the identity information was not considered equally reliable. Non-encrypted (http) websites continued to receive the “normal” browser UI (but no padlock), a difference that was barely noticeable to users. Here was the typical browser UI display at that time:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>No certificate (http)</td>
</tr>
<tr>
<td>2</td>
<td>DV or OV Certificate (DV certs <strong>without</strong> identity information – https) (OV certs <strong>with</strong> identity information - https)</td>
</tr>
</tbody>
</table>

(c) **Introduction of EV Certificates (2007).** By 2005 browsers recognized that stronger identity verification was needed, especially for websites that conduct significant revenue transactions or transfer sensitive data - there were no minimum authentication standards for OV certificates, and some DV certificates were being used for fraud. Over the next few years, a set of Extended Validation (EV) certificate guidelines was developed by the CA-Browser Forum, and the browsers upgraded their browser UIs to provide a distinct new security indicator for sites protected by EV certificates. Here is the typical browser UI hierarchy at that time for displaying different security states, including EV certificates:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Problem site</td>
</tr>
<tr>
<td>2</td>
<td>No certificate (http)</td>
</tr>
<tr>
<td>3</td>
<td>DV or OV Certificate (DV certs <strong>without</strong> identity information – https) (OV certs <strong>with</strong> identity information - https)</td>
</tr>
<tr>
<td>4</td>
<td>EV Certificate (EV – https with strongly confirmed identity information)</td>
</tr>
</tbody>
</table>

(d) **Lack of Common Browser UI Approach Causes Confusion.** Until roughly 2010, the browsers made an effort to coordinate their UIs using these security symbols so that users would understand what the symbols meant no matter what browser was used. A yellow padlock meant https/encrypted, a green padlock and green bar with identity information displayed meant stronger identity confirmation with an EV certificate.

Unfortunately, over time browsers no longer coordinated their UIs. Some of the leading browsers diverged in the signals they used to communicate security states – e.g., by using a green padlock for DV, OV, and EV certificates when the color green was previously reserved for EV certificates only. Indeed, some browsers modified their browser UI security indicators (color, position, etc.) with almost every new release. Today, it’s difficult to tell in some browsers which websites are protected by the highest level EV certificates, as opposed to which are protected by OV or DV certificates, because the use of the color green has spread to sites protected by all
types of certificates. Here are current examples from multiple browsers for http, https (DV and OV), and EV sites:

<table>
<thead>
<tr>
<th>Browser</th>
<th>HTTP</th>
<th>HTTPS</th>
<th>EV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chrome 48 Win</td>
<td><a href="http://www.exam1">www.exam1</a></td>
<td><a href="https://wv">https://wv</a></td>
<td>Symantec Co</td>
</tr>
<tr>
<td>Edge 20 Win</td>
<td>example.com</td>
<td><a href="https://ex">https://ex</a></td>
<td>Symantec Co</td>
</tr>
<tr>
<td>Firefox 44 Win</td>
<td>example.com</td>
<td><a href="http://www">http://www</a></td>
<td>Symantec Con</td>
</tr>
<tr>
<td>Safari 9 Mac</td>
<td>example.com</td>
<td>ssl://v</td>
<td>Symantec Con</td>
</tr>
<tr>
<td>Chrome 48 And</td>
<td><a href="http://www.example">www.example</a></td>
<td><a href="https://v">https://v</a></td>
<td></td>
</tr>
<tr>
<td>Opera Mini 14 And</td>
<td><a href="http://www.example">www.example</a></td>
<td><a href="https://v">https://v</a></td>
<td></td>
</tr>
<tr>
<td>UC Mini 10 And</td>
<td>Example Do.</td>
<td>ssl://v</td>
<td>Endpoint, C</td>
</tr>
<tr>
<td>UC Browser 2 iOS</td>
<td>Example Do.</td>
<td>ssl://v</td>
<td>Endpoint, C</td>
</tr>
<tr>
<td>Safari 9 iOS</td>
<td>example.com</td>
<td>ssl://v</td>
<td></td>
</tr>
</tbody>
</table>

There is also inconsistency between mobile and client security indicators. How can any user tell the difference between these different security states?

Noted TLS security expert Ivan Ristic commented on the confusion in browser UIs in his seminal book, *Bulletproof SSL and TLS (2016)* at pages 134-35:

Perhaps one of the contributing factors to the confusion is the lack of consistency, both among different browsers and in different versions of the same browser. User interface guidelines exist, but they are not specific enough.

I remember how in the early days of SSL there was a huge push to educate browser users about the meaning of the padlock (“If you see a padlock, you’re safe.”). A couple of years later, browser vendors started playing with the user interface. In some cases (e.g., Firefox), there were changes made with every new release. ***

Today, the only consistency, and only in the broad sense, is the use of green color for EV certificates. It’s still respected by all major browsers.

When it comes to mobile platforms, the situation seems to be worse. Due to much smaller screen sizes, browser vendors are trying to remove virtually all user interface elements, affecting security indicators in particular. With many mobile browsers, even security experts have a hard time distinguishing secure sites from insecure ones.

---

3 Taken from recent study “Rethinking Connection Security Indicators”,
4 https://securityintelligence.com/mobile-users-3-times-more-vulnerable-to-phishing-attacks/
This has led some researchers to conclude that mobile users are three times more vulnerable to phishing attacks. ***

As is apparent, current browser UIs are confusing, inconsistent, and constantly changing for a given browser, and don't adequately inform users of a site's security status. How can a user tell if an https site is DV, OV, or EV when all the symbols and colors are mixed together? Sadly, this was another missed opportunity – browsers could have rallied around and stayed with a few common UI implementations for EV certificates (just as they converged on the padlock years earlier for DV/OV) to help educate the public and avoid confusion. Such symbol standardization has been crucial for user safety in other areas, such as international traffic signs.\(^5\)

There is now an opportunity to improve and coordinate browser UIs as discussed below in Section 5 below.

2. **Analysis of Recent Developments**

(a) **Major Push toward Encryption.**

**Observations:** Major changes are occurring across the internet that will have a profound impact on the use of SSL/TLS and encryption - more than 50% of websites are now encrypted, and the number is rising rapidly. This is an opportunity to be seized for the benefit of users.

- Unencrypted http sites are now deemed unsafe for users because they are vulnerable to MITM attacks and don't protect user privacy. Browsers and sites are moving to “100% SSL” in stages. This creates added demand for the proper display of certificate-related information.

- New free DV certificate offerings such as Let’s Encrypt and others are helping the move to end-to-end encryption. Applications using Boulder-ACME-Certbot will help many site owners and hosting companies to install certificates on sites that were previously only http.

- Browsers may soon require https for websites to get a favorable UI security indicator – unencrypted sites will likely receive negative indicators. As a practical matter, this will push most sites to https as the “new normal.” Smaller steps toward this goal, such as boosting SEO rankings for site with a certificate and only supporting HTTP/2, the latest version of the protocol, are already in place.

**Conclusion:** These changes are all positive for user security, but they carry a risk as discussed below.

---

\(^5\) An example of a coordinated symbol understood by users around the world is the octagonal red “stop” sign used for traffic control. While the wording on the stop sign may be different in different countries, the stop sign is instantly recognizable to all. The stop sign was standardized across the US in 1935, and adopted internationally in 1968 under the Vienna Convention on Road Signs and Signals. [https://en.wikipedia.org/wiki/Stop_sign#Photo_Gallery](https://en.wikipedia.org/wiki/Stop_sign#Photo_Gallery) Similar UI standardization for certificate security states should be adopted by browsers and applications for protection of users.
(b) **DV, OV, and EV Certificates Will All Play an Important Role in the 100% Encryption Ecosystem**

There will be an important role for DV, OV, and EV certificates in a “100% encryption” ecosystem – but they will be very distinct roles, and each unique role should be uniquely recognized by the browsers. Here is a ranking chart showing the best use for each type of certificate in a 100% encryption internet:

<table>
<thead>
<tr>
<th>Certificate Type</th>
<th>Best Used For</th>
<th>Comments</th>
</tr>
</thead>
</table>
| DV               | Running your own web server for your own personal use  
Development and testing  
Internal company websites | May be favored for malware and fraud for reasons discussed below |
| OV               | Small business “brochure ware” website  
Web services (computer talking to external computer)  
Blogs | Likely to be used less for malware and fraud – see discussion below.  
Better protection when users providing information, better recourse from problem sites |
| EV               | E-commerce  
Banking  
Medical / highly sensitive information  
Sites susceptible to phishing | Safest form of certificate because of extensive authentication |

The PCI Security Standards Council recommends the use of OV/EV certs as part of the Best Practices for Safe E-Commerce.⁶

**Conclusion**: While malware and fraud exploits may move to DV certificates in many cases to avoid future http warnings (see discussion below), for most websites simply moving from http to encryption, even with a DV certificate, is a great advance in user security. For many websites that do not accept user information, DV certificates will still be appropriate.

However, OV and EV certificates will be more appropriate for sites that accept user information, and each should get its own favorable browser UI so that users can make appropriate security choices.

(c) **Malware Exploits Are Moving to Encryption and Are Harder to Block; DV Certificates May Become the Default Choice for Fraudsters.**

**Observations**: For many years, the vast majority of malware and phishing sites used http – it was cheaper and allowed the bad actors to retain their anonymity. There were virtually no user attacks using https. That is now changing.

As browser UIs are modified to generate user alerts for unencrypted http sites (see discussion of new Google browser UI security indicators below), fraudsters have started to migrate from

⁶ [https://www.pcisecuritystandards.org/pdfs/best_practices_securing_ecommerce.pdf](https://www.pcisecuritystandards.org/pdfs/best_practices_securing_ecommerce.pdf)
http to https, which can easily be achieved with a free and anonymous DV certificate. Users, websites, and web app operators are told they are safer using https, and so are not well prepared for fighting malware exploits delivered over https. In fact, encryption can actually prevent many network-based antivirus and malware detection programs from working effectively, meaning the encrypted malware can more easily infect systems.

According to a recent SC Magazine article, the use of encryption to hide malware is increasing exponentially – up 58 times (5,800%) in 2015 alone - and is often hard to detect by typical enterprise security infrastructure. The article states:

“As much as encryption is an essential tool for securing individual and corporate data, security professionals continue to find that the rising use of encryption cuts both ways – it is as easily used by cybercriminals as it is by enterprises. A research report discovered command and control servers (C&C) that use SSL to disguise malware increased by 200 times last year.

“The researchers also found that SSL-cloaked traffic in C&C increased by 58 times. In a release, enterprise security solutions provider Blue Coat Systems said the research indicates ‘that SSL/TLS will be increasingly used in the future to hide attacks.’

“‘Our researchers’ findings reveal what many have long suspected – that SSL traffic as a primary channel for malware and exfiltration is dramatically increasing,’ Blue Coat Systems president and COO Michael Fey said, in a statement. ‘In light of these growing threats, many organizations have realized that the balance between network performance and proper SSL inspection is not as simple as they had been led to believe by many of their network security providers.’”

Another study by A10 Networks and Ponemon Institute found that nearly half of cyber-attacks this year have used malware hidden in encrypted traffic.

**Rising Use of Encryption Gives Malware a Perfect Place to Hide**

Nearly half of cyber-attacks this year have used malware hidden in encrypted traffic to evade detection.

In an ironic twist, A10 Networks has announced the results of an international study with the Ponemon Institute, revealing that the risk to financial services, healthcare and other industries stems from growing reliance on encryption technology.

A growing number of organizations are turning to encryption to keep their network data safe. But SSL encryption not only hides data traffic from would-be hackers, but also from common

---


See also [Major spike in Malware encryption, Blue Coat finds.](https://securitybrief.co.nz/story/major-spike-malware-encryption-blue-coat-finds/)

See also [Malware disguised by SSL traffic spikes over the last year - New research suggests encrypted traffic is becoming the go-to method for threat actors to hide malicious code](http://www.zdnet.com/article/malware-disguised-by-ssl-traffic-spikes-over-the-last-year/)


security tools. The encryption technology that is crucial to protecting sensitive data in transit, such as web transactions, emails and mobile apps, can also allow malware hiding inside that encrypted traffic to pass uninspected through an organization’s security framework.

At the same time, a full 80% of organizations do not inspect their SSL traffic, making it even easier for hackers to bypass existing defenses by using SSL-encrypted traffic to hide their attacks. For many security managers, the costs of inspecting this rising tide of encrypted traffic outweigh the benefits. ***

Other results included that the fact that only 42% of inbound web traffic and 32% of outbound traffic is encrypted; and of the public-sector organizations that had been attacked in the last 12 months, 43% believed those attacks used encryption to evade detection. ***

Hackers and malware abusers will commonly create fraudulent websites for the purposes of ID theft and account takeover. To add legitimacy to the website, they will add extensive graphics to mimic the real website and obtain an SSL certificate, which gives the user a visual indicator of security (the closed padlock). Here are recent examples of phishing sites set up with encryption using anonymous, free DV certificates:

![Recent free DV cert phishing example sites](image)

Cybercriminals go to the trouble of obtaining DV certificates because users have become conditioned to look for the padlock or “https” before conducting a transaction. Many of these fraudulent sites are up for only days or hours, which means that unlike legitimate business, which only has to apply for certificates once every few years, the criminals are doing so constantly with anonymous, free DV certificates. The need for a certificate will be even greater to avoid a nasty browser warning once browsers require encryption for every website.

Clearly, hackers and malware abusers can accomplish their goal of creating a safe-looking website by using any type of certificate from a trusted CA – DV, OV, or EV. But there are advantages to bad actors for using DV certificates as their default choice. First, a DV certificate is relatively easy to obtain – fast (because of minimal interaction between the bad actor and the CA – in fact, for DV certificates the process can be automated and anonymous) and cheap (often free). In comparison, an OV or EV certificate usually costs money and requires back-and-forth interaction with the subscriber to ensure identity verification and a human element to make sure they are not being mis-issued. Second, obtaining OV and EV certificates requires the bad actor to provide confirmed identity and contact information, which is tested by the issuing CA. Finally, an OV or EV certificate leaves a trail that can be followed back to the bad actor once the certificate is used on a website for phishing or fraud, and both the confirmed organization and the confirmed domain can be banned from future certificates. For all these
reasons, bad actors are most likely to prefer DV certificates if they must use encryption to avoid an http warning in the browser.

Once the fraudster has purchased the rights to a domain, it can apply and easily receive a DV certificate. The website is then set up, and the fraudster will begin directing unsuspecting consumers to the site. Consumers will see the padlock (which DV certificates enable) and may proceed to enter private data which can be distributed through the criminal network.

Is there any evidence that fraudsters are, in fact, choosing DV certificates over OV or EV certificates today? Yes – the website SSL Blacklist (https://sslbl.abuse.ch/) provides a list of SSL sites that are associated with malware or botnet activities. A review of their most recent list indicates that all of the blacklisted SSL certificates are either DV or self-signed (note: self-signed or untrusted certificates incur a browser warning, which fraudsters will likely avoid).

On the evidence to date, DV certificates are preferred by fraudsters when moving from http to https, and OV and EV certificates are avoided. This is not to say DV certificates should not be trusted – they should, for the uses listed above – but only that they should not be used on websites where users are asked to provide passwords or personal or financial information.

As a separate matter, a limited number of fraudsters are obtaining certificates for deceptive domain names that look like high-value, legitimate domains – their goal is to trick users into thinking they are at a legitimate website. According to Netcraft:

“One Certificate authorities issue SSL certificates to fraudsters

“In just one month, certificate authorities have issued hundreds of SSL certificates for deceptive domain names used in phishing attacks. SSL certificates lend an additional air of authenticity to phishing sites, causing the victims' browsers to display a padlock icon to indicate a secure connection. Despite industry requirements for increased vetting of high-risk requests, many fraudsters slip through the net, obtaining SSL certificates for domain names such as banskfamerica.com***, ssl-paypai-inc.com***, and paypwil.com***.

“CloudFlare, a content delivery network that provides free "Universal SSL" to its customers, is a hotspot for deceptive certificates, accounting for 40% of SSL certificates used by phishing attacks with deceptive domain names during August 2015. CloudFlare's Universal SSL certificates are provided [in partnership with a CA], and CloudFlare also use [other CA] certificates for some of its customers. CloudFlare's flexible SSL option also appeals to fraudsters, offering a padlock in victims' browsers without the need for attackers to set up SSL on their web servers.***

“The CA/Browser Forum's Baseline Requirements – a set of rules that publicly-trusted certificate authorities are expected to follow – require that high-risk domain names that may be used for fraud or phishing are subjected to additional verification:


10Certificate authorities issue SSL certificates to fraudsters
See also The weakness of Domain Validated SSL certificates https://www.openprovider.co.uk/about-openprovider/news/the-weakness-of-domain-validated-ssl-certificates
“High-Risk Certificate Request: A Request that the CA flags for additional scrutiny by reference to internal criteria and databases maintained by the CA, which may include names at higher risk for phishing or other fraudulent usage.

“The CA SHALL develop, maintain, and implement documented procedures that identify and require additional verification activity for High-Risk Certificate Requests prior to the Certificate’s approval. ***

“The requirement to perform additional verification of high-risk certificate requests applies to all levels of assurance. However, DV certificates are often issued completely automatically within minutes, making it easy for fraudsters to obtain DV certificates for deceptive domain names. ***

“Despite this requirement, many major certificate authorities issue SSL certificates for deceptive domains used in phishing attacks.”

Conclusion: Fraudsters have already moved rapidly to DV certificates to gain more credibility for their phishing and malware sites and to evade enterprise and client security software. Also, some fraudsters have been able to obtain deceptive domain names that look like high-value, legitimate domains. Under current rules, CAs are required to implement systems for additional scrutiny of defined “High Risk Security Requests” such as deceptive domains. If a CA’s systems for reviewing High Risk Security Requests are not strong enough, a fraudster can potentially get a certificate for highly deceptive domains. CA’s need to step up and improve their systems to deal with the increasing use of https by fraudsters.

(d) Many browsers no longer do effective revocation checking, and some CAs no longer do certificate revocation for encrypted malware sites, so users are not as protected as in the past.

Observations: Because of competition and performance issues, and a concern that revocation checking might be blocked by MITM attacks, browsers have effectively dropped revocation checking for most certificates.

11 However, once a fraudster gets an OV certificate for a particular organization name that the CA has found in third party data bases like Hoover’s and Dun & Bradstreet (and confirmed the fraudster can be reached at the phone number or address found in the reliable third party data bases), that organization name will be entered on various blacklists and may not be able to obtain additional OV certificates for the same organization name in the future. It can take months or years to get an organization entry into these third party data bases, and the data bases use their own algorithms to look for fraud before publishing any information. What this means is that obtaining OV certificates for fraudulent look-alike domain names is not attractive to fraudsters – it takes too much work and too much time to be worthwhile. In general, they will prefer DV certificates, even for their deceptive high value domain names.

12 Browsers could greatly improve revocation checking by OCSP responder if they simply program their browser to do a “second tap” when revocation checking – first have the client browser request a revocation checking response, then if no response is received within a set time (milliseconds) submit a second OCSP response for the same URL before rendering the page to the user. In the vast majority of cases, a “second tap” will generate an OCSP response within acceptable latency periods. As a second safeguard, if the client browser fails to get an OCSP response on the second try, the website’s certificate should be downgraded in the browser UI to show as DV, even if the certificate is an OV or EV certificate. This simple change would solve most revocation checking problems and restore user security.
Here is the conclusion from a 2015 academic study measuring browser revocation checking.13

“*** CONCLUDING DISCUSSION

“Certificate revocation is a necessary component of any PKI, but it comes with costs, both real and perceived: CAs carry the cost of disseminating revocation information, while browsers risk the cost of increased web page load times. In the trade-off between low communication overheads and security, both ends of certificate revocation (those who issue and those who fetch) are naturally tempted towards the former. Indeed, the very utility of revocations has been debated and doubted [citation omitted] by the security community, but to date, these debates have had to largely depend on anecdotal CA and browser behavior.

“We have presented in this paper an empirical measurement of the options at all parties' disposal - website administrators, CAs, and browsers - in terms of the communication overhead costs they impose and the extent to which they are currently being employed.

“Overall, our results show that, in today's Web's PKI, there is extensive inaction with respect to certificate revocation. While many certificates are revoked (over 8% of fresh certificates and almost 1% of alive certificates), many web browsers either fail to check certificate revocation information or soft-fail by accepting a certificate if revocation information is unavailable.

“On the positive side, our results also demonstrate that there are several clear paths to improvement. To reduce CRL sizes, CAs can simply maintain more, smaller CRLs (in the extreme, each certificate could be assigned a unique CRL, resulting in an approximation of OCSP) - surprisingly few CAs currently take such an approach [citation omitted] and therefore incur greater bandwidth costs than strictly necessary. A promising improvement is OCSP Stapling, as it reduces CA bandwidth costs as well as web page load times - yet, not all browsers support it, and some that do simply ignore the responses. A more pervasive deployment of OCSP Stapling, at both websites and browsers, could lead to an immediate improvement in user security at little additional performance cost, particularly if the Multiple OCSP Staple Extension [citation omitted] were adopted to allow intermediate certificates to be stapled. Finally, we show that a straightforward modification to CRLSets could increase their coverage by several orders of magnitude.

“From these results, we conclude that certificate revocation ought not be given up on - that indeed it serves a critical yet overlooked role that, with proper support from all parties, can be achieved at a cost far outweighed by the benefits. To realize this, we believe continued measurement and validation of future browsers will be of utmost importance, and to this end have made our data and our browser test suite publicly available at http://www.sslresearch.org.” [Emphasis supplied.]

In addition, at least one major DV certificate provider no longer responds to certificate revocation requests for phishing and malware websites.

Let's Encrypt has issued millions of DV certificates since its launch in 2015, and now is a leading provider of DV certificates in the world.14 In early 2016, a leading security research lab

discovered that Let’s Encrypt certificates were being used by websites shown to be injecting malware, and the lab notified Let’s Encrypt with specifics. Let’s Encrypt responded by stating that as a matter of policy, it will not investigate or revoke certificates reported to it for malware exploits, even reports from a major research lab. Instead, Let’s Encrypt’s policy is to continue issuing free DV certificates to a known and reported malware site until someone reports the site to Google’s Safe Browsing application (after which Let’s Encrypt will not issue any new certificates to the domain) – but many malware sites never get reported in this way and so can continue to get free DV certificates forever. Also, Let’s Encrypt does not revoke previously issued certificates for sites that are reported to Google’s Safe Browsing, but instead will only refuse to issue renewal certs for those malware sites – which leaves the fraudsters in business for the full 90-day validity period for Let’s Encrypt’s free DV certificates.

In its posted policy on why it will not revoke certificates for phishing and malware reported websites, Let’s Encrypt states that “CAs make poor content watchdogs,” and even though phishing and malware sites are bad “we’re not sure that certificate issuance (at least for Domain Validation) is the right level on which to be policing phishing and malware sites ***.” The post continues that “Treating a DV certificate as a kind of ‘seal of approval’ for a site’s content is problematic for several reasons”, including that CAs are not well-positioned to operate anti-phishing and anti-malware operations and would do better to leave those actions to the browser website filters because of their greater access to data about dangerous websites and the rapidly changing nature of phishing and malware sites.

The Let’s Encrypt policy statement continues “Another issue with treating DV certificates as a ‘seal of approval’ for site content is that there is no standard for CA anti-phishing and anti-malware measures beyond a simple blacklist of high-value domains, so enforcement is inconsistent across the thousands of CAs trusted by major browsers.” The policy statement concludes “The fight against phishing and malware content is an important one, but it does not make sense for CAs to be on the front lines, at least when it comes to DV certificates.” (See entire statement at the URL in the footnote 16 above for a complete statement of Let’s Encrypt’s policy on revocation.)

**Conclusion:** Let’s Encrypt’s stated policy is at odds with what most CAs do (they respond to reports of their certificates being used on bad websites), but the policy makes one important point – that **DV certificates, in particular**, should not be viewed as a “seal of approval” to users concerning to a website’s safety or reputation, even in a 100% encrypted web. In that respect, perhaps revocation of DV certificates is not as important.

---

17 In fact, many phishing and malware sites simply abandon an old URL and move on to new URLs within Let’s Encrypt’s 90-day free DV certificate validity period, and so never even try to renew their DV certificate with Let’s Encrypt. For this reason, even if a malware site is reported to and listed on Google Safe Browsing list after has received a Let’s Encrypt DV certificate, that report will have no practical effect when the same fraudster comes back to Let’s Encrypt to get a new DV certificate for a new and different URL after the first certificate expires.
However, this same conclusion does not apply to the need for revocation of bad OV and EV certificates. Because OV and EV certificates can be relied upon as a proxy for user safety (see discussion at Section 4) and should receive distinct and favorable browser UI security indicators to distinguish them from DV certificates, the revocation of certificates reported for phishing or malware is very important to keep OV and EV certificates safe for users. Browsers may be able to solve their revocation checking problem by doing a “second tap” (resend a request for an OCSP response in milliseconds) as suggested at footnote 12 above. The CA-Browser Forum Baseline Requirements should continue to require CAs to respond to reports of their OV and EV certificates (at a minimum) being used on bad websites, and to respond by revoking the certificates if appropriate. This is another way to improve the reliability of OV and EV certificates for user safety.\footnote{If CA revocation requirements are dropped for DV certificates but continued for OV and EV certificates, this could greatly reduce the burden of revocation checking for browsers, as there are many more DV certificates than OV or EV – perhaps this distinction could be a part of the solution to revive revocation checking by browsers.}

(e) Users Assume All Encrypted Sites with Padlock Are “Safe” Sites.

\textit{Observations:} According to a recent Datamation article quoted below,\footnote{\textit{Let’s Encrypt: The Good and the Bad - The Let’s Encrypt initiative is a well-intentioned security solution, yet it does prompt some questions.} \url{http://www.datamation.com/security/lets-encrypt-the-good-and-the-bad.html}} users who see that a site is encrypted (even with only a DV certificate) may think the https and padlock means they are “safer” than with non-encrypted sites, but in fact all the padlock means is that communications with the site (even communications with https websites that engage in phishing or inject malware) are encrypted:

“\textit{The biggest problem with [the display of DV certificates in the browser UI] is that it democratizes access to https for any website. Yes, on the surface, this should, in fact, be a positive thing that we're celebrating. Unfortunately, human nature comes into play here. When most people (non-geeks/non-IT) see https, immediate and unwavering trust is implied.}"

“\textit{Even though [DV certificates are] merely providing encryption for your website, most people visiting it will give it the same level of trust as websites with the "green bar" https (Extended Domain Validation), which includes the company name next to the padlock in the address bar.}"

“\textit{This means that even though identity isn't actually verified at the same level as a green bar https website, most site visitors won't really know the difference. This is terrifying, and we should be concerned about this. What most people don't realize is that a secure connection to an untrustworthy website doesn't mean it's safe to use.}"

“\textit{To add further concern, there's very little preventing malware distributors from using [DV] certificates to make malware distribution websites look more official. Not only has it happened already, worse, is the fact that [DV certificate providers’] stance on this issue is quite weak.}"

“\textit{The initiative is putting far too much trust into the general public's understanding as to how https actually works. Fun fact folks – most people are clueless about tech. And the reality is merely comparing new registrations with Google's records won't be enough. Perhaps the blame for education needs to fall with the browsers instead?}”
As “100% encryption” becomes a reality enforced by the browsers, malware and phishing sites will migrate to free DV certificates offered by many CAs to avoid being blocked by the browsers, and users will not be prepared, but will generally avoid OV and EV certificates. According to a 2015 InfoWorld article:20

“*** Criminals simply need a marginally believable URL and a padlock icon displayed prominently in the browser to set up a successful phishing site. And domain-validated certificates are issued automatically within minutes, making them popular. ***

“Even if it isn’t up to the certificate authorities to fix the phishing problem, they can make it harder for fraudsters to get valid certificates. Netcraft’s analysis found [two named CAs’] certificates were not used by phishing sites, most likely because these two certificate authorities do not offer domain-validated certificates.”

Conclusion: As the article points out, phishing sites are getting certificates from many CAs that offer DV certificates,21 and are avoiding getting certificates from CAs that don’t offer DV certificates (most likely because they can get a DV certificate easier, and also because phishers didn’t want to provide OV or EV identity information when getting their certificates).22

(f) Browser Website Filters Expand, But Are Not a Complete Solution for User Safety.

Observations: Some have suggested that only DV certificates are needed for user safety, and that other user protections such as use of OV and EV certificates, certificate revocation, and even additional high-risk screening by CAs are unnecessary, because users can be adequately protected if they simply use applications such as Microsoft’s SmartScreen or Google’s Safe Browsing. This is not quite true for several reasons.

Microsoft SmartScreen has two main components – a phishing filter that may warn users if suspected phishing sites have been encountered,23 and a “Certificate Reputation” service that

---

21 See also Netcraft’s study of the “Phishiest Certificate Authorities” showing that virtually all CAs that issue DV certificates have issued some to fraudsters. http://toolbar.netcraft.com/stats/certificateAuthorities
22 While there is little evidence that OV certificates are being used by fraudsters to secure their websites, some code signing certificates that include identity information have been used by fraudsters to sign malware. In many cases, these malware code signing certificates have been issued to individuals, not to organizations, following the individual validated or “IV” certificates authentication procedures of BR 3.2.3. Unfortunately, BR 3.2.3 an IV certificate can be issued based solely on a pdf of a driver’s license (which can be easily faked) plus a confirming phone call to a one-use, “burner” phone, yet IV Certificates are treated as equivalent to OV certificates. If OV certificates receive a more favorable browser UI security indicator than DV certificates, as proposed by this White Paper, and IV Certificates also receive the OV browser UI security indicator, some fraudsters can be expected to move from DV certificates to IV certificates as a result. This would be unfortunate, given the weak authentication methods used when issuing IV certificates. As a result, IV certificates should not be treated as equivalent to OV certificates, and should not receive the new OV browser UI security indicator, until the IV certificate authentication methods are strengthened – they should be treated as equivalent to DV certificates until then.
23 https://en.wikipedia.org/wiki/Microsoft_SmartScreen
notifies a website owner when an unexpected certificate (different from the certificate found on a prior visit, and so potentially fraudulent) is found on its website so the website owner may request revocation if the certificate is bad.\(^\text{24}\)

SmartScreen has been found to be very effective in blocking access to sites containing security risks and malware downloads. In a September 2011 blog post, Microsoft stated that 1.5 billion attempted malware attacks and over 150 million attempted phishing attacks have been stopped.

However, there are some limitations with Microsoft SmartScreen.\(^\text{25}\) Users can’t report phishing URLs via an online form, but must click the suspicious URL and visit the website to use Internet Explorer's "report this website" feature. This potentially exposes the user to possible drive-by downloads or other malicious content in order to report the phishing website. Users cannot use non-Microsoft web browsers to report phishing URLs to Microsoft. Also, SmartScreen filters can be bypassed - some phishing attacks use a phishing email linking to a front-end URL not in the Microsoft database; clicking this URL in the email redirects the user to the malicious site. The "report this website" option in Internet Explorer only reports the currently-open page; the front-end URL in the phishing attack cannot be reported to Microsoft and remains accessible.

**Google Safe Browsing** is a blacklist service that provides lists of URLs for web resources that contain malware or phishing content.\(^\text{26}\) Google Chrome, Apple Safari and Mozilla Firefox use the lists for checking pages against potential threats. Google also provides a public API for the service and information to Internet service providers by sending e-mail alerts to autonomous system operators regarding threats hosted on their networks.

However, Safe Browsing does present some privacy issues involving cookies and maintaining browsing records from the same device. Safe Browsing warns users via popup if a URL is known as a potential phishing or malware site, but users can click through the warnings. Also, Safe Browsing only protects users if the Safe Browsing is turned on, and not all dangerous sites are listed – in fact, the malware injection sites listed in the article at footnote 17 above were never included in the Safe Browsing list of dangerous sites. Safe Browsing also relies on proprietary Google blocking algorithms, and so is not transparent to users.\(^\text{27}\)

Here are recent examples of phishing and malware sites not detected by Microsoft SmartScreen and Google Safe Browsing (URLs altered for safety):\(^\text{28}\)

---


25 [https://en.wikipedia.org/wiki/Microsoft_SmartScreen#Criticism](https://en.wikipedia.org/wiki/Microsoft_SmartScreen#Criticism)

26 [https://www.google.com/transparencyreport/safebrowsing/](https://www.google.com/transparencyreport/safebrowsing/)


28 **Source:** Comodo Valkyrie malware analysis system  
Conclusion: Microsoft SmartScreen and Google Safe Browsing clearly provide a strong service and should be used, but they are not a complete or real-time solution for user safety and may not be available to many users, especially around the world. Under certain conditions, the service may be interrupted by MITM attacks. Even though these solutions are free, they are not built into all clients, and no one can expect all clients to build them in. Also, it remains to be seen how effective these website filtering applications will be as fraudsters move their sites to 100% encryption.

There is one simple answer that uses existing, widespread security SSL/TLS infrastructure: leverage the existing confirmed identity information in OV and EV certificates as a proxy for user safety. Using the type of SSL/TLS certificate securing a website as a proxy for user safety can convey important information to users even before a website is reported to Microsoft or Google for malware or phishing, or before there is ever a request for certificate revocation – a huge advantage.

User safety should be provided in depth, with multiple layers of defense including anti-malware and security software on users’ devices and all enterprise systems, browser website filter applications, encryption via digital certificates which are revoked for malware, certificate revocation checking, and special reliance on certificates with identity information (OV and EV certificates) as a proxy for user safety, as discussed below.

(g) New Chrome Browser UI Announced; Disappearance of Certificate Identity Data.

Observations: At least one browser (Google) has announced it will soon require https on websites to receive the “normal” UI state (padlock), and Google has completely redesigned its browser UI security indicators as discussed below.²⁹ However, as noted in subsection (d) above Chrome does not check for certificate revocation status for most websites, and Google representatives have stated that Google may soon stop making OV certificate identity information available to users.³⁰

²⁹ Rethinking Connection Security Indicators.  
³⁰ As noted in the study at Footnote 13 above, Google and other browsers have dropped most revocation checking of certificates. For example, Google’s internal list of revoked certificates, CRLsets, covers only 0.35% of revoked certificates, meaning that the remaining 99.65% of revoked certificates show as “good” in Chrome. Google has
With its redesign, there are only three browser UI states displayed in Chrome, starting with Chrome 52 for Mac desktop and Chrome 53 for other platforms. (For now, EV certificates will still receive an EV “green bar” in Chrome with identity information for a fourth browser UI state, but as discussed below Chrome might drop any special display for EV certificates in the future, treating them as the equivalent of DV and OV for browser UI security purposes.) Here are the three new UI states:

stated its future intention to eliminate the ability to click through to identity information in OV certificates in Chrome at meetings of the CA/Browser Forum.
1. Security Indicator for HTTPS - encrypted sites (but with no distinction between DV and OV certificates) – “Secure”

![Secure Indicator](image)

2. Security Indicator for HTTP only - no encryption – “Not secure”

![Not Secure Indicator](image)

3. Security Indicator for Invalid HTTPS - encrypted but with mistakes – “Not secure”

![Not Secure Indicator](image)

(Note that both the gray circle-“i” indicator and the red triangle-exclamation point indicator are shown by Chrome as “Not Secure,” but presumably the red indicator is intended to mean especially “Not Secure.”)

The new Chrome UI security indicators are presented in the study referenced at Footnote 3 above. Here is Google’s conclusion:

“We evaluated forty icons and seven complementary strings by surveying thousands of Google Consumer Survey respondents. Ultimately, we selected and proposed three indicators: a Secure for HTTPS, ⊗ Not secure for HTTP, and ▲ Not secure for invalid HTTPS. Our proposed indicators have been adopted by Chrome, and we hope to motivate others to update their security indicators as well. Our next step is to evaluate the indicators internationally, once they have been in use for several months.”

As to the future, it’s not clear whether or not Chrome will continue to display EV certificates to users with the distinctive green bar and confirmed identity information displayed to users in the browser UI, as it does at present. The same Google study also stated the following about https generally, and about EV certificates in particular:
“In the past, HTTPS was viewed as a sign of website trustworthiness; getting a valid HTTPS certificate was too difficult for typical phishing websites. Dhamiya et al. challenged 22 people to identify phishing websites, and 17 of them failed to check the connection security indicator during the study [citation omitted]. This demonstrated that connection security indicators were ineffective at preventing phishing attacks. Subsequently, HTTPS has ceased to be a useful signal for identifying phishing websites because it is no longer unusual to find malicious websites that support HTTPS. We, therefore, do not aim to use HTTPS as an anti-phishing defense.

“EV is an anti-phishing defense, although its use is limited by lack of support from popular websites and some major mobile browsers. All major desktop browsers display EV information, but some mobile browsers (including Chrome and Opera for Android) do not display EV information. Older literature suggests that EV indicators may need improvement. Jackson et al. asked study participants to identify phishing attacks and found that “extended validation did not help users defend against either attack” [citation omitted]. When testing new security indicators, Sobey et al. concluded that Firefox 3’s EV indicators did not influence decision making for online purchases [citation omitted]. Improving EV indicators are out of scope for our current work.”

Google engineers have stated in meetings that users don’t value or understand EV certificates, and that Google might eliminate all browser UI differentiation for EV certificates in the future. If this occurs, EV certificates would effectively be downgraded in Chrome and treated the same as DV and OV certificates, meaning that the distinctive green bar and confirmed identity information displayed in the browser UI would disappear. This would effectively mean Chrome presents only a binary UI – only Good (“Secure,” with one indicator and no way to distinguish between DV, OV, or EV or know if website identity information is present) and Bad (“Not Secure,” with two indicators). This would be a real security setback for users.

There is a significant danger to users from a simple binary UI – users will have no way to tell the difference between a fake DV phishing site for a high-value target such as the PayPal login page from a real EV site – the actual PayPal login page. Here’s a recent example.

This is how the unencrypted http phishing site www.paypal.com.summary-spport.com appears in Chrome (the SLDN controlled by the phisher in highlighted in red):

![Chrome UI Security Indicator](image)

The Chrome UI security indicator is just a gray circle-

Once Chrome shows security warnings for http sites that have password login fields, it will display warnings to the user. This phisher was able to obtain an anonymous, free DV certificate for its domain www.paypal.com.summary-spport.com – see how that changes its Chrome UI security indicator to a green padlock and the words “Secure,” which all sites with DV certificates
receive. Notice also that because of the small image size, the phisher’s SLDN summary-support.com has disappeared from the URL line – instead, all a user sees is the 3rd and 4th level domains for this certificate, paypal.com:

![Phishing login page](image)

Clearly, users are going to be tricked into thinking this is the real PayPal login page because of the green padlock and the words “Secure.”

Now, this is the real PayPal login page, secured by an EV certificate. Notice the slight differences from the DV secured phishing page above:

![Real PayPal login page](image)

At least Chrome displays the actual company name Paypal and nationality [US] confirmed by a certificate authority from multiple sources to differentiate it from a DV certificate – but both sites have the green padlock, and users may find it hard to tell the difference in Chrome between DV and EV certificates.

That’s not the end of the example – what will happen if Google actually does eliminate the special EV certificate browser UI, and truly goes to a simple, binary security UI for Chrome “Secure” and “Not Secure”? When that happens, all https websites will look exactly the same, and users won’t know which are DV and which are EV with strongly confirmed identity information. Both the fake DV phishing login page at www.paypal.com.summary-support.com and the real PayPal EV login page at www.paypal.com will look exactly the same, with the following Chrome UI:
This will truly put users at risk.

Chrome also recently removed the ability of users to click on the Chrome padlock to see the identity information contained inside OV and EV certificates. Instead, the ability to see certificate identity information is available only in the “developers” version of Chrome. This decision effectively hides all site owner identity information from interested users.

The Google study noted that both experts and non-experts expressed confusion about the meaning of current browser UI security indicators as to the security of a website, and presented the following encouraging conclusion:

“We did learn, however, that understanding security icons is not impossible for non-experts. Nearly all of our extension survey respondents associated Chrome’s green lock with HTTPS and security. Their beliefs — particularly around identity — were not always complete or correct, but they still understand the general concept of the indicator. Although these respondents were tech-savvy, they were not security experts, which makes us hopeful that others will also learn the meanings of indicators with sufficient nudges.”

The study’s Concluding Summary includes the following call to action to other browsers:

“Chrome will launch our proposed connection security indicators with Chrome 53. However, we hope that our indicators are not limited to Chrome’s URL bar. We would like to see other products that convey connection security adopt similar shapes to reinforce the meaning of the indicators. All of the icons are free to use as part of Material Design. ***

“Our proposed indicators have been adopted by Chrome, and we hope to motivate others to update their security indicators as well.”

Google’s encouragement to others to adopt the new Chrome UI security indicators was re-emphasized in a message to subscribers to the Google security-dev@chromium.org list on July 26, 2016, where Google stated it would use its red triangle-exclamation point symbol to flag “malicious and deceptive” sites listed in Google Safe Browsing, and again encouraged other browsers to adopt the same security indicators for greater user understanding. The statement says:

“*** We plan to add the dangerous security state icon [red triangle] on malicious and deceptive sites that are flagged by Google Safe Browsing. These icon improvements are the first step in an overhaul of how Chrome communicates connection security state.

“We conducted extensive user research to choose these indicators, and we’ve shared our results in a peer-reviewed scientific paper. If you’re a developer who needs to communicate connection security, we encourage you to use the same icons from Material Design to convey the same security states as Chrome, and to secure your site with HTTPS if you have not done so already.”

Finally, in September 2016 Google modified its plans for these new security indicators, and stated it would gradually substitute the red triangle warning “Not Secure” icon for unencrypted http sites, instead of using the gray circle-“i” icon for http sites as stated in its June 2016 paper.31 The red triangle warning will first be applied to http sites with password or credit card

31 https://security.googleblog.com/2016_09_01_archive.html (Sept. 8, 2016)
form fields in January 2017, with Chrome 56. In following releases, Google will continue to extend the red triangle warnings to other uses of http - for example, by labeling http pages as “not secure” in Incognito mode, where users may have higher expectations of privacy. Eventually, Google plans to label all http pages as non-secure, and change the http security indicator to the red triangle that it uses now for broken https.

**Conclusion:** Here are a few preliminary conclusions about Google’s recent UI redesign:

- Google has made a good start in creating better security status UI indicators, and is correct that browsers and other applications should collaborate and use common UI indicators to avoid user confusion (compare to the inconsistency and confusion for current browser UIs in the table shown in Section 2(d) above). Google should be congratulated for this suggestion and for its design ideas.

- However, Google is continuing to treat DV and OV certificates as equivalent in its new browser UI. For reasons discussed below, this is missing an opportunity to make use of identity information to protect users.

- Unfortunately, Google’s new browser UI security indicators continue to use a green padlock for DV and OV certificates as well as for EV certificates, instead of the original yellow or grey padlock used for many years by most browsers for DV and OV certificates. Green padlocks were originally introduced as a distinction reserved for the highest level EV certificate, along with the obvious green bar and identity information. Using green for all three levels of certificates (DV, OV, and EV) will cause user confusion – which is what Google says it wants to avoid.

- If OV and EV certificates no longer have a market because they are effectively downgraded to the same browser UI security indicator, then those products will be discontinued by CAs, and much of the identity verification ecosystem developed over 20 years that has supported them will be permanently destroyed – and once the authentication infrastructure is gone, it will be gone for good and won’t come back. Is this a wise step?

- Google’s September 2016 announcement that all http will eventually be downgraded to the red triangle “Not Secure” icon is a great decision and one that will help us reach 100% encryption as early as possible.

---

32 In the future, after OV certificates receive their own distinctive browser UI security indicator, it would be wise for Google to extend this decision and require that http sites with password or credit card form fields are secured by an OV certificate, not a DV certificate, to help protect users against fraudsters with a DV certificate.

33 One question – normally the use of the letter “i” as a symbol is positive or neutral, indicating the availability of useful information, such as at travel offices in cities and pop-up instruction guides and KBAs on websites. In this case, Google is using the letter “i” in a gray circle as a negative warning to users that a site is http only and so is “Not Secure”, which is the same status shown for malware sights with the red triangle and exclamation point. Was this a wise choice? Users probably start with an expectation that the letter “i” represents something positive or neutral but useful, and may become confused to see it used as a negative warning “Not Secure” in the Chrome UI similar to Chrome’s red triangle. This question will be resolved eventually when Chrome uses the red triangle warning for all http sites (same symbol as for broken https), which is a good move.
Finally and optimistically, the Google study states that users don’t really understand the meaning of the current confusing UI security indicators, but correctly concludes that it may be possible for non-security expert users to "learn the meanings of indicators with sufficient nudges." This can include learning the importance of identity in certificates in a 100% encrypted web if the users are allowed to know that the identity information is there for them to use. (That is, nudges can also be used to train users on the differences between DV, OV, and EV certificates, as discussed below.)

3. **Employing Certificate Identity Information as a Proxy for User Safety.**

So here is the dilemma – 100% encryption represents a major advance for the Internet, as it protects user privacy and can guard against MITM attacks. But encryption itself does not make a site trustworthy, it can hide malware, and it can fool users into thinking they are safe just because they see a padlock or other indicators of encryption. The use of DV certificates by fraudsters is surging. What to do?

There is one simple answer that uses existing, widespread security TLS infrastructure: *leverage the existing confirmed identity information in OV and EV certificates as a proxy for user safety.* Using the type of SSL/TLS certificate securing a website as a proxy for user safety can convey important information to users even before a website is reported to Microsoft or Google for malware of phishing, or before there is ever a request for certificate revocation – a huge advantage.

Studies and common sense show that virtually all fraudsters (malware, phishing, etc.) will use DV certificates for their websites to respond to the requirement of 100% encryption, as they can get the certificates for free and will receive the same browser UI security indicators as an OV certificate. Because fraudsters stick with DV certificates, that means OV and EV certificates are associated with substantially lower fraud rates and so represent user safety.34

On this basis, browsers should modify their current UI security indicators to tell users when a website is https secured using confirmed identity information – OV or EV certificates – as opposed to sites that are secured using anonymous DV certificates. Uniform identity authentication procedures are already in widespread use by CAs worldwide, and OV and EV certificates are already securing responsible websites used for ecommerce and sensitive financial or personal information.35 The 25% of encrypted websites with OV and EV certificates today are much safer for users than the 75% of anonymous websites with only DV certificates.

---

34 In the rare case where a fraudster uses an OV certificate for phishing or malware, CAs and law enforcement will have identity and contact information that can be used to track the fraudster down, and can blacklist the organization name in the O field of the certificate to prevent the fraudster from ever getting another OV certificates for different domains. As noted in footnote 11 above, it is very hard and time consuming for a fraudster to establish a new organization identity is a third party data base, and those data bases do their own fraud checks.

35 Does this mean DV certificates are bad and shouldn’t be used because they are favored by fraudsters? Not at all – DV certificates remain the fastest, easiest means of securing a website, and are entirely appropriate for many uses. But they should no longer be used for ecommerce or other sensitive information sites because of the threat from fraudsters who are moving to DV certificates as browsers require encryption for a “normal” UI.
In essence, confirmed website identity information in existing OV certificates is a great, unmined treasure trove that can now be used by browsers to protect users against the coming onslaught of fraud perpetrated by DV encrypted websites. Browsers should give websites with OV certificates better a superior browser user interface than websites with only DV certificates, and should use the confirmed identity information in OV certificates in their algorithms (e.g., Microsoft SmartScreen and Google Safe Browsing) to protect their users. OV identity information has never been used effectively by applications over the past 20 years. To choose not to use this data makes no sense.

Here is the chain of logic we follow:

- Browsers are pushing website owners to 100% encryption (that’s good)
- Fraudsters are rushing to free DV certs to hide (that’s bad)
- DV certs are often free, allow anonymity, provide no identity or recourse
- OV and EV certs include identity, allow recourse – almost no fraud or phishing has been recorded for OV, none for EV
- But, users can’t tell the difference between DV and OV certs – both receive the same UI in the browsers; and EV may be downgraded to the same level as DV and OV by Chrome in future release
- Conclusion: We are wasting valuable identity information already inside OV and EV certs – we should use confirmed identity as a proxy for user safety

Fortunately, there is a relatively easy solution that would not require any major browser UI redesign, but instead simply reassigns existing browser UI security indicators.

## 5. A Proposal for Reassignment and Redesign of Current Browser UI Indicators to Promote Identity and User Safety

As noted above, fraudsters prefer to preserve their anonymity when launching malware and phishing exploits. DV certificates allow them to maintain perfect anonymity, and so defeat some of the benefits of the current move to 100% encryption by the browsers.

As noted above, fraudsters avoid OV and EV certificates because they don’t want to identify themselves for potential law enforcement efforts, and prefer the fast and cheap (and often free) issuance of DV certificates to enable encryption of their short-lived sites to avoid user warnings. So a simple solution is to use identity information in OV and EV certificate as a proxy for identifying safer sites that are much less likely to be used for malware and exploits. At the same time, OV and EV certificates provide verified identity information to users and law enforcement if they want to use that information.

### 2016 Data

<table>
<thead>
<tr>
<th>Type</th>
<th>Number (000s)</th>
<th>Percent</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>DV</td>
<td>7,503</td>
<td>75%</td>
<td></td>
</tr>
<tr>
<td>OV</td>
<td>2,353</td>
<td>24%</td>
<td>25%</td>
</tr>
<tr>
<td>EV</td>
<td>243</td>
<td>1%</td>
<td></td>
</tr>
</tbody>
</table>

Source: Frost and Sullivan
How can certificate identity information in OV and EV certificates be used as a proxy? By giving each level of certificate an increasingly favorable browser UI display. This translates as “OV is better than DV,” and “EV [because of the more detailed identity authorization] is better than OV.”

The browser UIs should reflect this increasing level of safety so users can understand which sites are the safest. Even if users choose not to look at the actual identity information in an OV or EV certificate, they can make intelligent safety decisions about different websites if they see a different UI for each level of certificate. That’s not possible today because DV and OV certificates are treated as equivalent in the browsers, and EV certificates may be stripped of their distinct UI presentation in the near future as well.

(a) Getting to a browser UI that differentiates DV, OV, and EV certificates.

We know from previous discussions with browser designers that it is extremely difficult to make any significant changes to browser UIs, and such changes are only possible when strongly justified by new information or needs. But a simple reassignment of existing browser UI security indicators could be relatively easy.

All website owners are being pushed from http to https but not all websites can comply immediately, so there should probably be no change in the short term. However, once the web reaches an encrypted level of, say, 85-95% of websites, there will no longer be a need to show a padlock symbol for basic https (DV certificates), and in fact, DV secured sites should simply receive the lowest “normal” UI in a browser. This means the padlock symbol can be reassigned to OV certificate secured sites as an indicator of greater user security – identification plus encryption together.36 Users have been trained for years to “look for the padlock for safety,” so browsers should leverage that training in their new designs promoting website identity.

Browser UIs could revert to old designs and reassign security symbols (e.g., warnings for http, no indicator for DV, gold padlock for OV, green padlock and bar with identity information for EV), but it makes more sense to leverage the new and improved security symbols from Google and other browsers instead. By way of example, here are both the current browser UI security indicators for Google and Apple, plus two alternative future designs that could be implemented once 85% to 95% of websites have moved to encryption – this will give the industry time to educate website owners and help them prepare.

(1) Current Browser UI Security Indicators

Here are the current UI indicators for Google Chrome (including its new design) and Apple Safari (first screen shot), and for Microsoft Edge and Mozilla Firefox (second screen shot). (Note: the Chrome screen shots are for Chrome release 56, as it will appear in January 2017, and we have used Google Chrome on Mac for these images because the new Chrome indicators were released first for Macs.)

---

36 As the saying goes, “What good does it do to have encrypted communications if you don’t know who you are communicating with?”
Current Google Chrome and Apple Safari UI Security Indicators

<table>
<thead>
<tr>
<th></th>
<th>Google Chrome</th>
<th>Safari</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTPS EV</td>
<td>![Citigroup Inc. [US]</td>
<td><a href="https://online.citi.com">https://online.citi.com</a>](<a href="https://online.citi.com">https://online.citi.com</a>)</td>
</tr>
<tr>
<td>HTTPS (DV &amp; OV)</td>
<td>![Secure]</td>
<td><a href="https://www.google.com">www.google.com</a></td>
</tr>
<tr>
<td>HTTP &amp; Minor Security Issues</td>
<td>![Not secure]</td>
<td><a href="https://www.example.com">www.example.com</a></td>
</tr>
<tr>
<td>Broken HTTPS</td>
<td>![Not secure]</td>
<td><a href="https://www.example.com">www.example.com</a></td>
</tr>
</tbody>
</table>

Observations:

Google Chrome has both positive and negative security indicators. These help to:

- Encourage encryption and higher levels of transparent identification, and
- Punish bad SSL security practices.

Apple Safari has the simplest security indicators and is arguably the easiest to understand, but it offers only positive security indicators to users and doesn’t distinguish between http and major and minor security issues. Apple also uses a gray padlock (not green) for DV and OV certificates, which may be a better solution to differentiate them from EV certificates.

The primary change between the existing Chrome UI and the Chrome release 56 UI set for January 2017 is that Google will introduce a grey “Not secure” warning for HTTP for web pages with password and credit card fields that are not protected by a web server certificate and for minor security issues. Other http sites will simply get a grey circle-i indicator for now. Also, a red triangle and red “Not secure” warning will appear for Broken HTTPS websites. Eventually, Google Chrome will mark all HTTP and broken HTTPS sites with the same “Not secure” red warning triangle.

The UI also adds the word “Secure” in green text for both DV and OV certificates that arguably makes these vetting levels seem stronger than the EV vetting level, which does not display the word “Secure.” This change seem counter to the goal of creating a more secure and intuitive Internet for users.

Neither Google nor Apple distinguishes between DV and OV certificates at the present time. That should be remedied in future browser UI designs for the reasons stated in this paper.
Current Microsoft Edge and Mozilla Firefox UI Security Indicators

<table>
<thead>
<tr>
<th></th>
<th>Microsoft Edge</th>
<th>Firefox</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTPS EV</td>
<td>[🔒 Citigroup Inc. [US]] citi.com</td>
<td>[🔒 Citigroup Inc. (US)] <a href="https://online.citi.com/US/login">https://online.citi.com/US/login</a></td>
</tr>
<tr>
<td>HTTPS (DV &amp; OV)</td>
<td>[🔒 google.com]</td>
<td>[🔒 <a href="https://www.google.com/?gws_rd=ssl">https://www.google.com/?gws_rd=ssl</a></td>
</tr>
<tr>
<td>HTTP &amp; Minor Security Issues</td>
<td>example.com</td>
<td>[ℹ️ <a href="http://www.example.com">www.example.com</a>]</td>
</tr>
<tr>
<td>Broken HTTPS</td>
<td>[ℹ️ expired.badssl.com]</td>
<td>[ℹ️ <a href="https://expired.badssl.com">https://expired.badssl.com</a>]</td>
</tr>
</tbody>
</table>

Observations:

Microsoft and Firefox currently have similar user interfaces, but Microsoft Edge provides more distinction between the (combined DV and OV) state versus the EV state—it’s the grey outline lock symbol. Firefox’s use of the green lock symbol for both DV, OV and EV diminishes the difference between the three verification states, and could be potentially confusing to users, while Microsoft’s user interface encourages more EV with its user interface and therefore encourages websites to upgrade to its highest level of transparent identification.

None of Google, Apple, Microsoft nor Firefox distinguishes between DV and OV certificates at the present time. That should be remedied in future browser UI designs for the reasons stated in this paper.

Clearly a lot of knowledge and hard work by browser experts goes into their UI design, and the alternative browser UI proposal presented below is not meant to replace all the good design decisions made by browsers in the past and shown above. However, we believe there are certain key principles that are important to any browser UI security design, including (1) presenting information and meaningful distinctions to users to allow them to make their own security choices, and (2) presenting user security information in a consistent manner (including coordination among browsers to avoid user confusion) so that users can learn what indicators mean as they move across devices, whether a laptop running IE, Edge, or Chrome, an iPhone running Safari or Firefox, or an Amazon tablet – there must be consistency across all these user environments.

With those principles in mind, here is an alternative proposal for new UI security indicators.

(2) Alternative browser UIs after web reaches 50%-65% encryption – DV and OV distinguished

Here is a proposed reassignment of the Google, Apple, Microsoft, and Firefox browser UI security indicators once the web reaches 50%-65% encryption that would distinguish between DV and OV certificates for the first time as a proxy for user safety.
Potential Future **Google Chrome and Apple Safari** UI Security Indicators after Web Reaches 50%-65% Encryption

<table>
<thead>
<tr>
<th>Google Chrome</th>
<th>Safari</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTPS OV</td>
<td><a href="http://www.google.com">www.google.com</a></td>
</tr>
<tr>
<td>HTTPS DV &amp; Minor Security Issues</td>
<td><a href="http://www.example.com">www.example.com</a></td>
</tr>
<tr>
<td>HTTP &amp; Broken HTTPS</td>
<td>□ Not secure</td>
</tr>
</tbody>
</table>

Potential Future **Microsoft Edge and Mozilla Firefox** UI Security Indicators after Web Reaches 50%-65% Encryption

<table>
<thead>
<tr>
<th>Microsoft Edge</th>
<th>Firefox</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTPS OV</td>
<td>citi.com</td>
</tr>
<tr>
<td>HTTPS DV &amp; Minor Security Issues</td>
<td>example.com</td>
</tr>
<tr>
<td>HTTP &amp; Broken HTTPS</td>
<td>□ badssl.com</td>
</tr>
</tbody>
</table>

**Observations:**

- HTTP and HTTPS protocols (i.e., the letters http: and https:) are no longer displayed in the address bar if all sites are required to be encrypted. This frees up space.
- This proposal adds a Country flag indicator to the Apple EV UI to better indicate organization jurisdiction.
- On the Google Chrome indicator, the word “Secure” is removed, because eventually all sites will need to be secured by a web server certificate or else they will receive a “Not Secure” indicator in Chrome. Adding the word “Secure” at that time for sites secured by a certificate would be redundant.
- This proposal also modifies the Google indicator for OV certificates from a green padlock to a gray or black padlock to avoid confusion with EV certificates.
- It also adds to the current Apple UI to show a *negative* security result for the first time—a red domain URL that is crossed out for unencrypted and broken HTTPS sites.
This proposal promotes higher levels of vetted certificates with both trust indicator and color differences, thereby providing an incentive for website owners to move to higher levels of authentication to achieve a more prominent, favorable UI.

The designs for Google and Apple in the image above each have pros and cons. The Chrome design contains more information, while the Safari design can be used on both desktops and mobile devices because it has a smaller footprint.

This proposed alternative browser UI design helps reach the following common goals:

- Once adopted, it creates enhanced pressure on the last remaining 35-50% of unencrypted websites sites to serve encrypted (https) sessions.
- It encourages sites to identify themselves to the highest possible level of authentication appropriate for the website’s needs.
- Finally, it presents a cleaner UI among the browsers.

(3) Possible Future “Universal” Browser UI Security Indicators Shared by All Major Browsers

Finally, based on these principals for how current browser UI security indicators could be changed after the web reaches 50%-65% encryption (section (b) above), here is a proposal for a possible future “universal” set of browser UI security indicators that could be shared by all major browsers across all device types (laptop and mobile devices) to avoid user confusion. (As Google’s seminal browser UI security indicator study from June 2016 concluded, all browsers should work together to come up with common indicators to help users understand what they mean – see footnote 3 above.)

Potential Future “Universal” Browser UI Security Indicators

<table>
<thead>
<tr>
<th>Universal Browser UI – Ideal for Desktop and Mobile</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTPS EV</td>
</tr>
<tr>
<td>➕ Citigroup Inc. [US]</td>
</tr>
<tr>
<td>HTTPS OV</td>
</tr>
<tr>
<td>➕ bing.com</td>
</tr>
<tr>
<td>HTTPS DV &amp; Minor Security Issues</td>
</tr>
<tr>
<td>example.com</td>
</tr>
<tr>
<td>HTTP &amp; Broken HTTPS</td>
</tr>
<tr>
<td>➠ Not secure</td>
</tr>
</tbody>
</table>

Design by Chris Bailey

Here are potential concepts for design of a future “Universal” set of browser UI security indicators to be shared by all major browsers.

- Reserve green colors for **EV certificates**, including the green lock, e.g.
Microsoft has done a good job in visually separating DV/OV from EV certificates today by using both a grey lock and black text as well as a grey “lock outline” graphic, e.g.

This form of security indicator should be reserved for OV certificates in a future Universal set of browser UI security indicators.

Consider a neutral state for DV certificates, e.g.

telease.com

Once encryption is required in order to avoid a negative UI warning, there is no longer any reason to show a security indicator for a site encrypted with a DV certificate – it would then be the minimum “normal” state for websites.

Finally, begin implementing a progressive series of negative UIs for HTTP only sites and poorly configured HTTPS sites. Again, browsers can move from Phase 1 through Phases 2 and 3 (increasingly severe security warnings) for http sites as a greater and greater percentage of the web is encrypted. Here is one possible set of progressive negative UI warnings that could be used in a Universal set of browser UI security indicators:

- Phase 1 - 🔄 Not secure | www.example.com
- Phase 2 - 🔄 Not secure | www.example.com
- Phase 3 - 🔄 Not secure

Consider standardizing icons, font, colors and minimum data elements to show only the minimum required information in a way users can understand no matter which browser or device they are using.

These Universal browser UI principles would lead to security indicators that are simple and occupy the least space possible (important in the mobile environment) and can be easily understood by users across all devices and browsers. In any event, if the principle browsers would now form a working committee of their own to design common Universal browser UI security indicators (with input from Certifications Authorities and the public), it would be a great advance for user safety.

Rewarding website owners who take the trouble to provide identity information and be vetted to the OV level (by giving them a favorable UI that distinguishes from DV certificates) would incentivize them to authenticate to the higher level above DV, just as the favorable EV browser does today. That should be the joint goal of CAs and browsers – persuading website owners to
provide the most confirmed identity information about their websites to provide more data for browser safety algorithms and to protect users.

(b) Can Users Be Educated in the Symbol Reassignment?

Such a reassignment of browser UI hierarchy would be a great advance for user safety, and the symbol meanings would be relatively easy to convey to users once standardized across multiple browsers and applications. As the Google study concludes at its own footnote 18:

“We did learn, however, that understanding security icons is not impossible for non-experts. Nearly all of our extension survey respondents associated Chrome’s green lock with HTTPS and security. Their beliefs — particularly around identity — were not always complete or correct, but they still understand the general concept of the indicator. Although these respondents were tech-savvy, they were not security experts, which makes us hopeful that others will also learn the meanings of indicators with sufficient nudges.”

Joint education efforts among CAs and browsers could provide effective “nudges” to users to look for the gray or green padlock (symbolizing an OV or EV certificate with confirmed identity information) as a sign of greater user safety for a given website – which ironically is nearly the same basic message conveyed to users 20 years ago! The message to consumers for the Universal browser UI security symbols could be as simple as this:

- Always insist on encryption as a minimum requirement (this is enforced by browser warnings for http)
- Look for the “padlock” (which means OV or EV) before providing any personal information (password, credit card number) to a website
- Finally, look for the green bar (EV) for high security transactions, such as banking or health care matters

The short summary to consumers would be “look for the padlock!” which would mean OV or EV.

Do we need all browsers to adopt these common UI security indicators to succeed? No – while we would prefer that all browsers take a uniform stance, we can make major progress if even two browsers join together in using these new UI security indicators once the internet reaches 85%-95% encryption. At that point, new studies can test if users are actually safer with the new UIs versus browsers that don’t adopt the new UIs – if the answer is yes, that may encourage all browsers to come together and use the new security indicators.

(c) Summary and Conclusion.

In summary, user safety should be provided in depth, with multiple layers of defense including anti-malware and security software on users’ devices and all enterprise systems, browser website filter applications, encryption via digital certificates which are revoked for malware, certificate revocation checking, and special reliance on certificates with identity information (OV and EV certificates) as a proxy for user safety.

6. Additional Industry Steps to Strengthen Certificates and User Safety

Finally, CAs should not rest with this updated browser UI security indicator effort – there is more to be done to make encryption and SSL/TLS certificates more effective for user safety. These include the following initiatives:
1. Improve the OV identity authentication standards in the current CA-Browser Forum Baseline Requirements so that identity information in OV certificates is even stronger. As noted at footnote 22 above, this includes giving IV certificates only DV UI status until the IV authentication standards are greatly strengthened so that fraudsters don’t migrate from DV certificates to IV certificates in order to receive the benefit of a more favorable OV browser UI security indicator.

2. Improve the High Risk Certificate Request requirements in the Baseline Requirements (i.e. require additional scrutiny by CAs) to help reduce the issuance of certificates for deceptive, high value domains (e.g., paypa1.com, etc.). Note that this will not stop the bulk of phishing and malware sites from getting certificates to avoid the http warning, as most of these sites do not use deceptive, high-value domains.

3. Create improved information sharing procedures among CAs and browsers so that OV certificates can be blocked for organizations found to have used OV certificates on phishing and malware websites. This will greatly increase the safety of OV certificates, which are already considerably safer than DV certificates.

4. Because this browser UI security indicator redesign will place new emphasis on identity, we need to rethink some common practices involving OV and EV certificates.

Today, a hosting company can purchase a single OV or EV certificate with the hosting company’s organization name in the O field, but then add dozens of independent customer domains in the SANs fields belonging to other organizations that are using the hosting services. All that is required is for the hosting company to show control over the requested domains, which is easy for a hosting company to do. This could mislead users to think that the hosting company named in the OV certificate’s O field actually owns each website for the domains in the OV or EV certificate, which is not true. CAs and browsers should look for a solution so that the identity information in OV and EV certificates is not misleading to users.

5. Require all CAs to use the common DV, IV, OV, and EV common OIDs listed under BR 1.2 and EV Guideline 9.3.2 in order to make adoption of new, common browser UI security indicators that distinguish among these certificate types easier and more reliable. Microsoft’s Trusted Root Certificate Program already requires this, but use of the common OIDs should become a formal CA/Browser Forum requirement as well.

6. CAs should work together with browsers and server makers to increase use of OCSP stapling and introduce new slimmed-down CRL structures to make certificate revocation checking more robust and reliable, and browsers should experiment with improved revocation checking by making a “second tap” (a second request for an OCSP response within milliseconds if there is no response to a first request) and downgrading OV and EV pages to DV to protect users if no revocation checking response is received within an acceptable latency period. Even if revocation checking disappears for DV certificates (an unfortunate event), at a minimum revocation checking should be made more robust and be mandatory for 100% of OV and EV certificates, which represent greater user security.
7. Finally, CAs and browsers should jointly develop user education efforts around the new, common browser UI symbols once standardized across browsers so that users can spot the UI differences for different types of TLS certificates and understand what they mean for user safety.

These initiatives will be discussed in the CA Security Council in coming weeks (perhaps starting as a voluntary OV vetting “upgrade” initiative among the largest CAs for greater user safety), and their implementation will further justify the switch to new browser UI security indicators showing the difference between DV and OV certificates once the web reaches 85%-95% encryption.

7. **Five Principles of TLS Certificate Identity**

The arguments and conclusions of this White Paper are encompassed in the following *Five Principles of TLS Certificate Identity*, which are endorsed by all seven of the CA Security Council members listed below.

1. **Identity** in TLS server certs should be used by browsers as a proxy for greater user safety
2. CAs should vet their customers to the *highest identity level* possible
3. **OV certs** should receive their own browser UI different from DV certs to show user safety
4. **EV certs** should continue to receive a separate browser UI from OV and DV certs to show greater user safety
5. Browsers should agree on *common UI* security indicators, *avoid changes* to UI, and work with others to *educate users* about the meaning of the common UI security indicators for greater user safety.

Promoting TLS certificate identity is an exciting new project for us and will greatly improve user security as we move to a 100% encrypted web. For more information, visit [www.casecurity.org/identity](http://www.casecurity.org/identity).

[v1.0 15 Feb 2017]
Potential Future “Universal” Browser UI Security Indicators – Desktop and Mobile

<table>
<thead>
<tr>
<th>Universal Browser UI – Ideal for Desktop and Mobile</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTPS EV</td>
</tr>
<tr>
<td>![lock] Citigroup Inc. [US]</td>
</tr>
<tr>
<td>HTTPS OV</td>
</tr>
<tr>
<td>![lock] bing.com</td>
</tr>
<tr>
<td>HTTPS DV &amp; Minor Security Issues</td>
</tr>
<tr>
<td>example.com</td>
</tr>
<tr>
<td>HTTP &amp; Broken HTTPS</td>
</tr>
<tr>
<td>![alert] Not secure</td>
</tr>
</tbody>
</table>

*Design by Chris Bailey*