CA Security COUNCIL

A CA Security Council White Paper

EXECUTIVE SUMMARY

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

We are moving toward a 100% encrypted web – but can we get it right? We must leverage certificate identity data for greater user security.

1. Recommendation:

As websites move to 100% encryption, phishing and malware sites are hiding with legitimate websites by using anonymous, free DV certificates – they hate identity. Roughly 25% of websites are secured with OV and EV certificates that contain confirmed identity information, and virtually no OV or EV sites have ever been reported for phishing or malware.

Browsers have confused users by limiting and constantly changing browser UIs so users can't know whether a website's identity has been confirmed by an OV or EV certificate (and therefore is much safer for the user). To solve this problem, browsers should cooperate to create standard, "Universal" browser UI security indicators that indicate whether a website is secured by a DV, OV, or EV certificate, and should work with CAs and the media to educate users in the meaning of the new UI symbols.

2. Background:

There are three types of TLS certificates – DV or Domain Validated certificates, which are anonymous and contain no identity information about the website owner (and the issuing CA often has no information), OV or Organization Validated certificates, which contains identity information confirmed through simple vetting using reliable third party data and creation of a confirmed customer contact, and EV or Extended Validation certificates, which contains strong identity information through extensive vetting using reliable third party data and government registries, plus additional confirmed contact points with people at the customer organization.

Browsers today do not show any difference between DV and OV certificates, but typically present a favorable browser UI for EV certificates. But there are problems with browser UI security indicators, as discussed below. We propose a way to fix the UI for greater user security.

3. Positive Developments in Encryption

- There is a rapid move to encryption – over 50% of websites are now encrypted.

- Browsers are mandating encryption in stages (starting with webpages with login or credit card fields) – these pages must be *https* or they will receive a negative browser UI. This means *https* for all websites is becoming the "new normal" browser UI state.

- Encrypted sites receive higher SEO rankings, which is also pushing more sites to *https*.

- Automated certificate issuance and installation is taking off – Boulder, ACME, Certbot – making encryption easy for small users.

- Free DV certificate services – Let's Encrypt and others – encourage websites to try move to encryption.

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

But what good is encryption if you don't know *who* you're talking to?

4. Negative Developments in Encryption

- Malware exploits are moving to encryption to hide and avoid UI warnings for *http* sites. Once encrypted, these sites are harder to block.

- DV certificates are now the default choice for fraudsters – DV certificates are anonymous, free, and will gain the green "Secure" padlock in the browser UI, thereby avoiding the browser warnings that are coming for *http* sites. In addition, fraudsters can get DV certificates for "look-alike" names like the following recent examples of phishing sites secured with anonymous, free DV certificates:

Recent free DV cert phishing example sites	
paypal-4updates.com	net-flix.one
icloud-unlock.pl	amazom.ml
icloud-lostapple.info	paypal-security.center
www.verif-icloud.com	p.aypal.info
restore-amazon.com	safe-payment.online
intl-paypal.hotchat.online	portal-us-bankofamerica.com

- The DV padlock and word "Secure" in the browser UI is viewed by most users as meaning "safe," but that's not true now that phishing and malware sites are being pushed to encryption.

- Many browsers no longer do effective revocation checking, so even if DV certificates for phishing and malware sites are revoked, users will never be warned by the browser.

- Some CAs no longer revoke DV certificates reported for phishing or malware– they say "it's not my job."

- Browser website filters such as Microsoft SmartScreen and Google Safe Browsing are helpful for user security, but they are not a complete solution – thousands of phishing and malware sites are not included on the filter list.

What more can we do to protect users in the coming 100% encrypted environment?

5. Using Identity in Certificates as a Proxy for User Safety

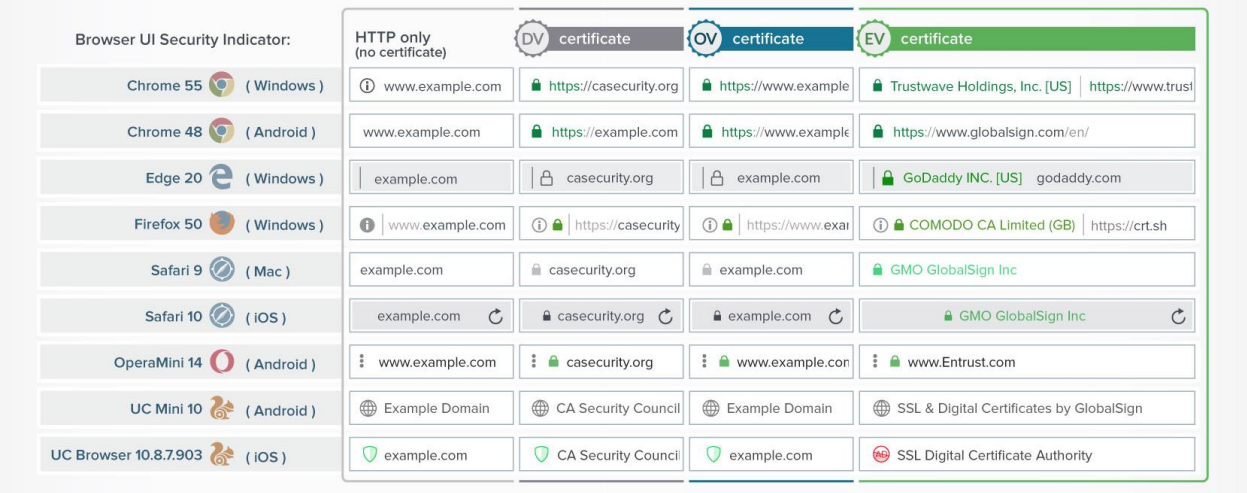
OV and EV certificate vetting uses reliable third party data bases plus government registries to confirm the identity of website owners, and also uses out of band communications based on third-party contact information to make certain they are communicating with the organizations they have vetted.

Phishing and malware sites hate identity – they will not use OV or EV certificates for their bad sites because of the time and expense involved, plus possible exposure and blacklisting for future OV and EV certificates if their websites are abusive. This means that OV and EV certificates (which secure 25% of all websites today) are much safer for users than sites secured by anonymous, free DV certificates. But current browser UI security indicators are a mess, and users can't tell which encrypted websites are secured by OV and EV certificates with confirmed identity, and which are secured by anonymous, free DV certificates (which has become the certificate of choice for fraudsters).

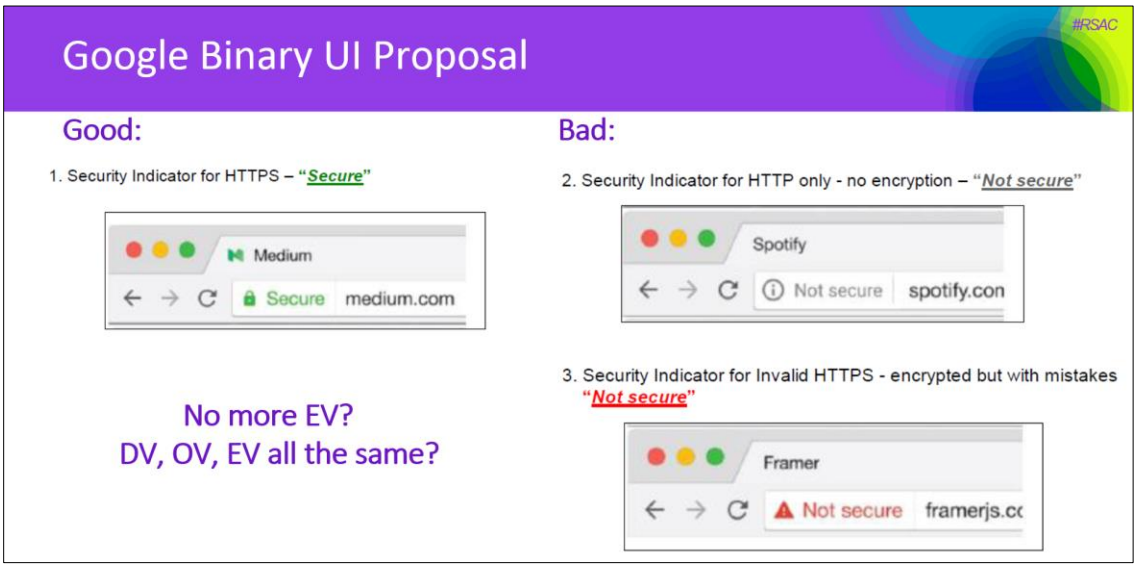
6. The Problems with Current Browser UI Security Indicators

Current browser UI security indicators are a mess:

- There is no consistency across browser UIs as to the four possible states for a website: unencrypted, DV, OV, and EV.
- Individual browsers frequently change their own UI, and users can't keep up.
- Browsers have added an array of other warnings to their UI (minor problems, major problems) that the average user doesn't understand.
- Most mobile devices don't even show any symbol for encryption or type of certificate.
- As a result, users are confused about how to read browser UIs – see following table. Who can understand what this means for any one browser, or across browsers?

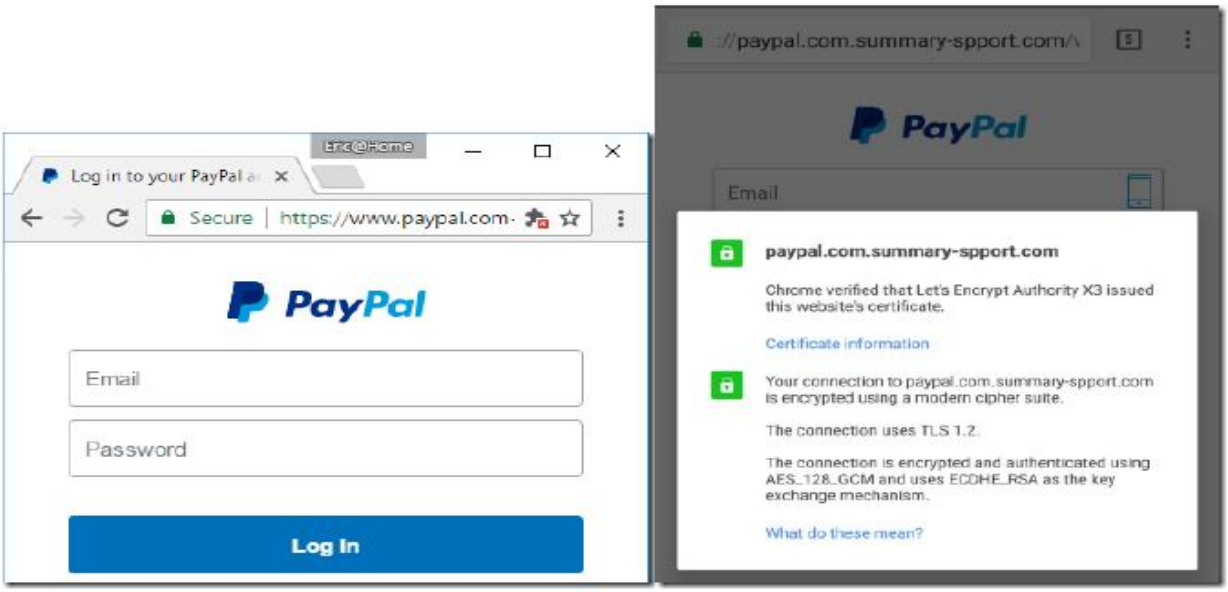


- Google may be moving to a simple, binary browser UI, with a green "**Secure**" (for DV, OV, and EV) and gray or red "**Not Secure**", with no indication whether a website is secured by a certificate with identity information – and may eliminate *any* EV certificate indicator from the Chrome UI:

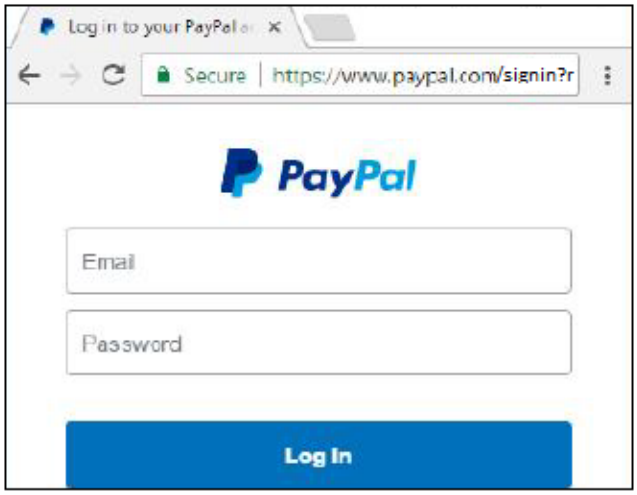


- If this happens, a fake PayPal login page for the domain *paypal.com.summary-spport.com* secured by an anonymous, free DV certificate will look essentially the *same* as the real PayPal login page *paypal.com/login* secured by an EV certificate. Compare:

Fake PayPal login site *paypal.com.summary-spport.com* secured with anonymous, free DV certificate:



Real PayPal login site *paypal.com/login* secured with EV certificate (if Chrome treats DV, OV, and EV certificates the same in its UI):



Users won't see any difference between the fake PayPal login site and the real login site, and will be fooled if all certificates (DV, OV, and EV) are treated as the same in the browser UIs.

7. How Should We Think About this Situation?

The chain of logic leading to a solution and greater user security is as follows:

- Browsers are pushing website owners to 100% encryption *(good).*
- Fraudsters are rushing to encryption using DV certificates to hide, avoid http warnings *(bad).*
- DV certificates are free, allow anonymity, no identity, no recourse for injured users.
- OV and EV certificates include identity, allow recourse for injured users – plus, there has been virtually no fraud or malware for OV sites, none for EV sites.
- But, *users can't tell the difference between DV and OV certificates* – both receive the same UI in the browsers today – and the EV certificate UI may be *downgraded* to the same level as DV and OV by Chrome in the near future, based on product plans.

Conclusion: *We are wasting valuable identity information already inside OV and EV certs* – we should use identity data in these certificates as a *proxy* for user safety.

8. How Do We Get to a Common Browser UI That Leverages Certificate Identity?

Start by adopting the following *Five Principles of TLS Certificate Identity:*

1. Identity in TLS server certificates should be used by browsers as a proxy for greater user safety
2. CAs should vet their customers to the highest identity level possible

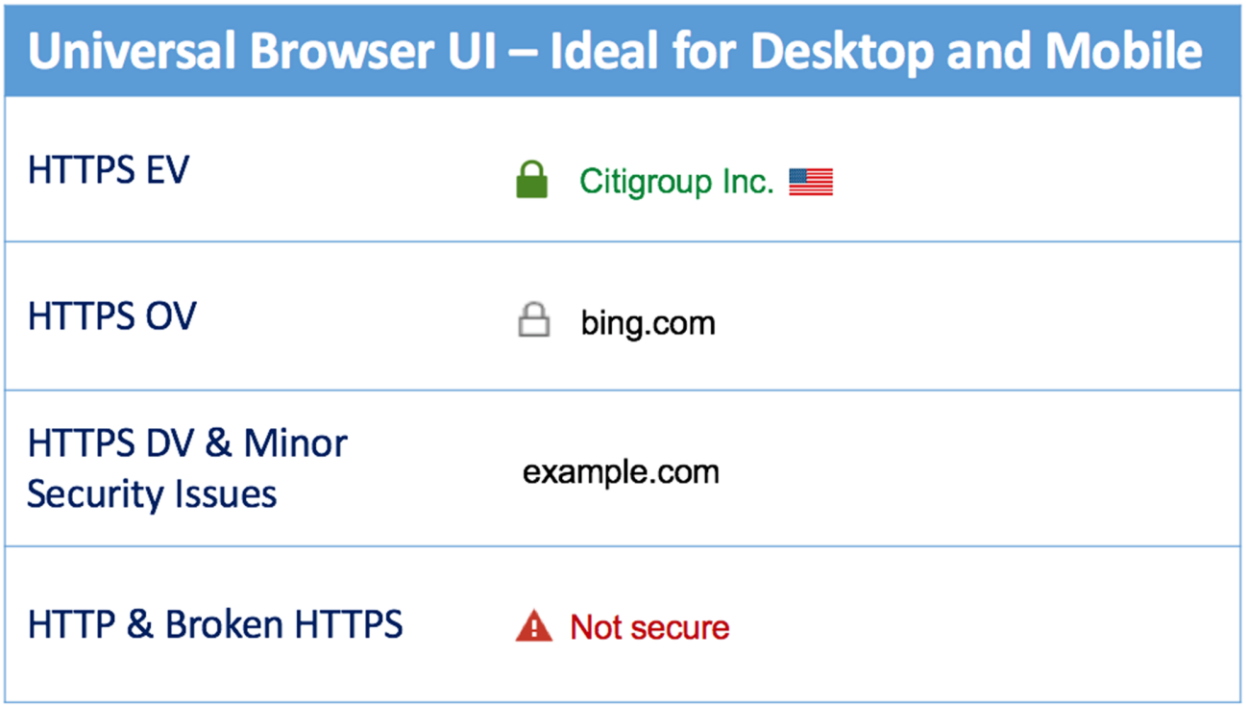
3. OV certificates should receive their own browser UI security indicator, different from DV certificates to show user safety

4. EV certificates should continue to receive a separate browser UI from OV and DV certificates 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.

These CAs and organizations have already endorsed the Five Principles of TLS Certificate Identity listed above, and more endorsements are on the way.

Here is an initial suggested design for a possible "Universal" browser UI that could be adopted by multiple browsers, one that would not be changed so that users can learn what the symbols mean for their security (*note:* this is just an initial suggestion for discussion by browsers and their UI developers):



Design by: Chris Bailey

9. Expected Obstacles and Responses to "Universal" Browser UI

We can expect the following objections to the idea of a "Universal" browser UI, and we offer the following responses:

- "Users don't understand the difference among DV, OV, and EV certificates and browser UIs."

  Response: That's because browsers keep changing their UIs, and there's no user education = user confusion.

- "OV vetting isn't rigorous enough for its own browser UI."

  Response: That's probably not true, but in any case, CAs standardized OV vetting rules in 2012 and will strengthen OV vetting even further as needed.

- "We browsers will decide safety for our users using internal algorithms – we may just move to a binary UI ("🔒 **Secure**" for all certificate types – DV, OV, and EV – and "Not Secure" for *http* and errors, and drop our current EV certificate UI)."

  Response: This may be Google Chrome's current approach – but it totally wastes available identity information in 25% of outstanding certificates that can enhance user security with very little effort by the browsers or others.

- "It's too hard to transition from current DV/OV single UI to new, separate OV UI."

  Response: Announce the change a year ahead – customers will migrate from DV certificates to OV and EV certificates to get the better UI once it's announced.

10. How Do We Train Users to Understand the New "Universal" UI?

First, reach general agreement on which type of certificate is most appropriate for which type of website. Here is one possible approach:

Cert type:	Best for:
DV	Running your own web server for your own personal use Web services (computer talking to internal computer) Development and testing Internal company websites
OV	Small business "brochure ware" website Web services (computer talking to external computer) Blog
EV	E-commerce Banking Medical / highly sensitive information Sites susceptible to phishing

Next, create simple rules for users – and everyone (browsers, CAs, the media) must work together to present a common user message, and repeat it often. Here is one possible simple message for users:

> **"Look for the warnings"** and insist on encryption as a minimum requirement (i.e., follow the *browser warnings* to avoid *http, broken https*)
>
> **"Look for the padlock in the address bar"** (OV or EV) before providing any *personal information* (password, credit card number) to a website
>
> **"Look for the green bar"** (EV) for *high-security transactions*, such as banking or health care matters

We successfully trained users to look for a padlock and an EV green bar ten years ago – we can train them again on how to use the new, common UI security indicators for their security.

11. Do Website Owners Support the Display of Website Identity?

Very much so (although no one ever asks website owners what they want in user security – they want a display of website identity to protect their brand and users).

Here are three *Website Identity Principles*, and a partial list of major enterprises that have given their endorsement to these Principles. Additional organizations may endorse these principles by signing up here: www.casecurity.org/identity

PUBLIC ENDORSEMENT OF WEBSITE IDENTITY PRINCIPLES

We, the undersigned organizations, strongly support the display of website identity for user security, and we specifically endorse the following website identity principles:

1. Website identity is important for user security.

2. TLS certificate types that are used to secure websites – Extended Validation (EV), Organization Validated (OV), and Domain Validated (DV) certificates – should each receive a distinct, clearly-defined browser UI security indicator showing users when a website's identity has been independently confirmed.

3. Browsers should adopt a common set of browser UI security indicators for each certificate type and should educate users on what the differences are to promote user security.

The following enterprises have endorsed these Website Identity Principles:

Source: Comodo and Entrust Datacard

12. What are the Next Steps for User Security?

- Browsers should collaborate and adopt a common "Universal" UI of their choosing
- Browsers should announce a transition date to new Universal UI
    - Unencrypted *http* websites will receive browser UI warnings
    - Padlock will disappear for DV, which will become the new "normal" state
    - OV certs will receive a new, distinct UI symbol
    - EV certs will continue with an enhanced EV UI symbol
- Start an education program to prepare users, website owners
- CAs should work on strengthening OV vetting, improved common standards
- All parties collect and respond to data on the use of certs by fraudsters (DV, OV, EV)

Result: A safer Internet for users within 1-2 years; fraud prevention.

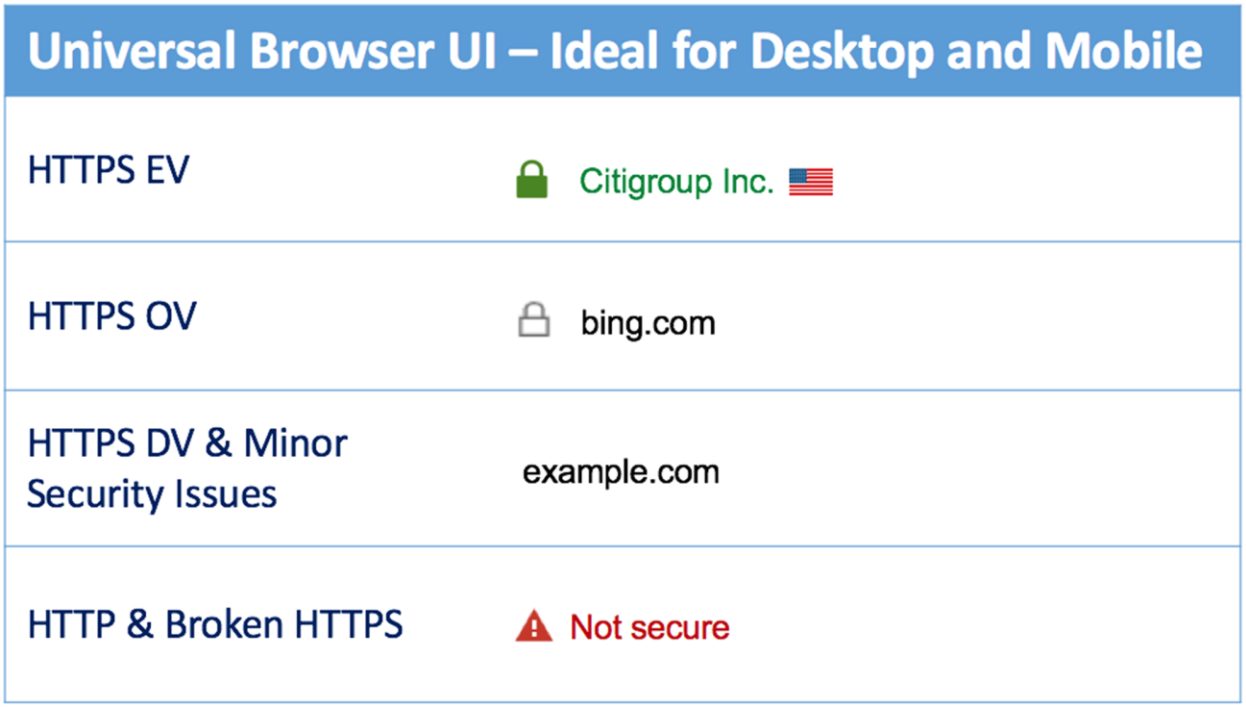
13. Final Summary

- Fraudsters are rapidly moving to DV certificates to avoid new *http* warnings and hiding among legitimate websites.
- Fraudsters hate identity – they avoid OV and EV certificates.
- Therefore, OV and EV certs (which are 25% of current websites) represent much *safer* sites for users – they can prevent internet crime.
- On this basis, *OV and EV certs deserve their own distinct browser UIs for user security.*
- Browsers should *not* eliminate the EV browser UI, and *should not* move to a binary UI of ("🔒 **Secure**" vs. "Not Secure"- that *hides* the identity information already contained inside OV and EV certificates that represent much safer websites.

- Browsers should work together to create a common Universal UI that users can understand, and *not* make frequent changes to their common UI.

- All parties – browsers, CAs, and the media - should work together to educate users on the new Universal UI

Here is a possible prototype "Universal" Browser UI one last time – this is just a starting point, and the UI experts at the browsers should apply their knowledge to create a better one.



Design by: Chris Bailey

For further details and supporting citations, see full version of White Paper *"Use of Identity in SSL-TLS Certificates for User Safety"* at www.casecurity.org/identity.