#RSAC

RSAConference2017

San Francisco | February 13 – 17 | Moscone Center

POWER OF OPPORTUNITY

SESSION ID: PDAC-W10

100% Encrypted Web New Challenges for TLS

Kirk Hall
Dir Policy & Compliance, Certificate Services
Entrust Datacard

RSA Conference2017

We are moving toward a 100% encrypted web – but can we get it right?

We must leverage certificate identity data for greater user security

We Will Discuss…

- Types of Server Certificates
- Past and Present Browser UI Security Indicators
- Positive Developments in Encryption
- Negative Developments in Encryption
- Using Identity in Certificates as a Proxy for User Safety
- How Do We Get to a Common Browser UI That Leverages Identity?
- Next Steps

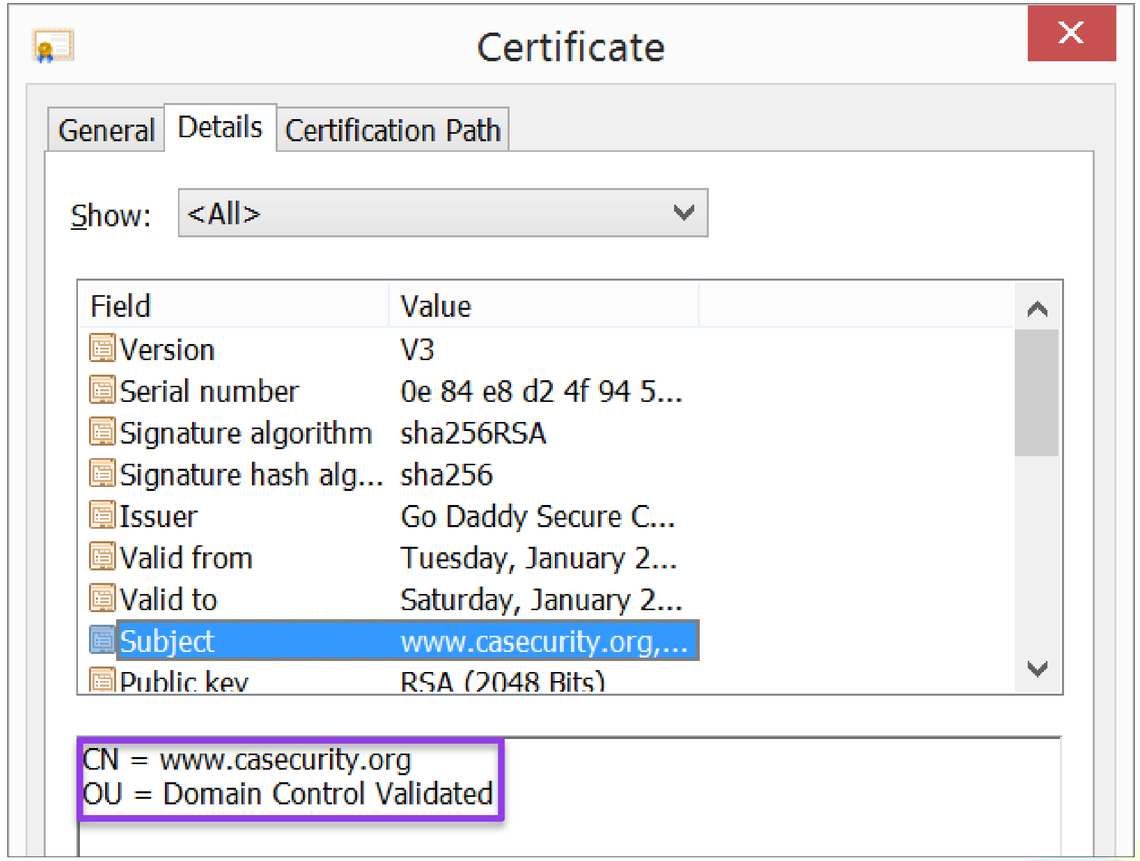
RSAConference2017

Types of Server Certificates

Digital Certificate Refresher

Types of Server Certificates

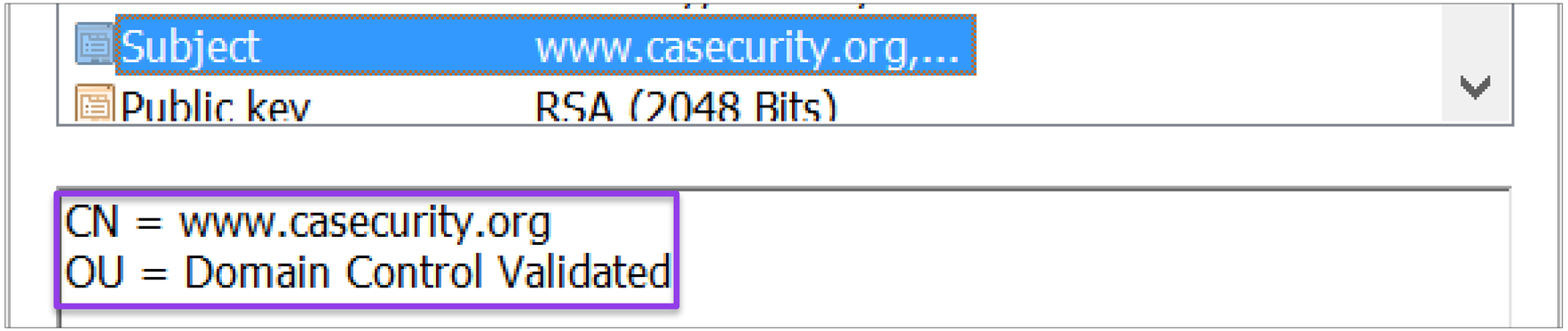
Domain Validated (DV) – No identity information, just a confirmed domain



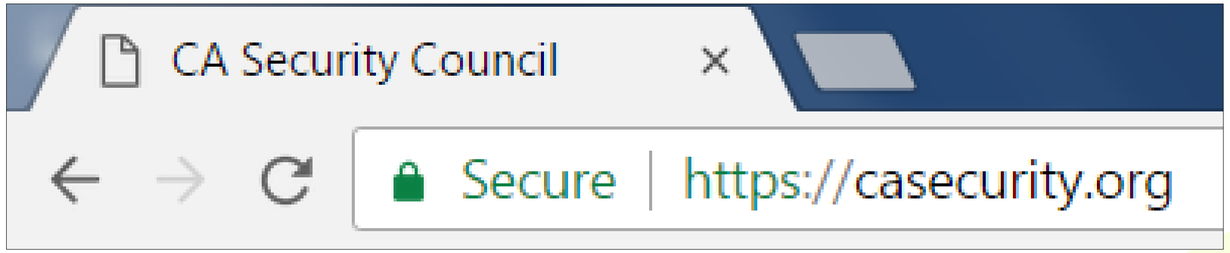
Types of Server Certificates

Domain Validated (DV)

Close Up:

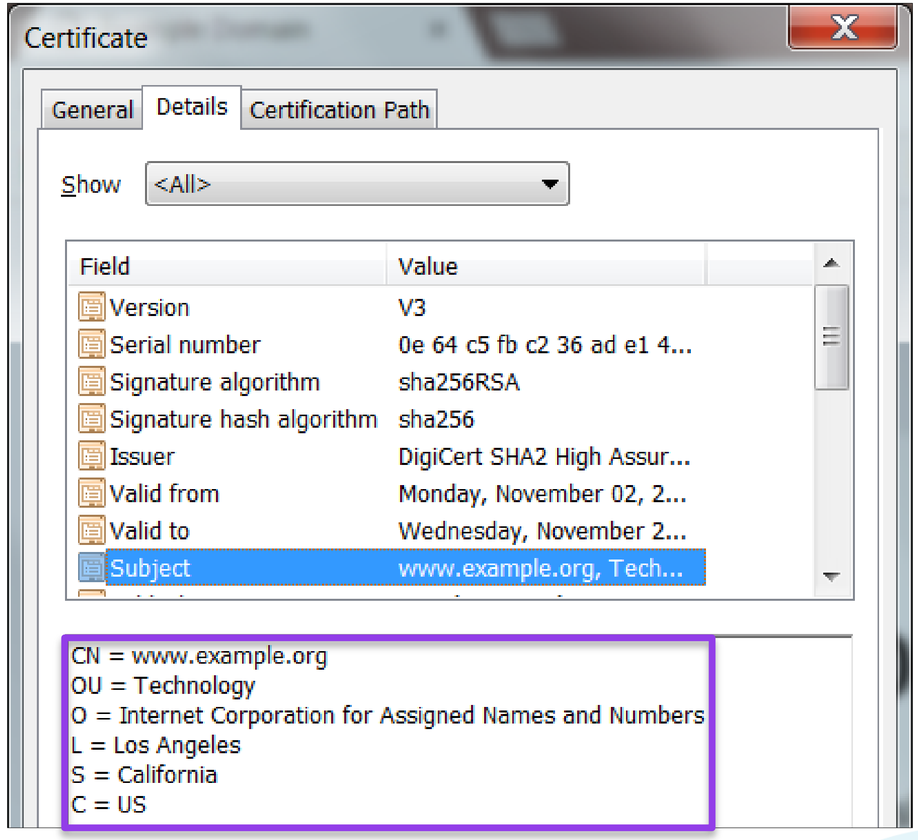


Sample Browser Treatment (Chrome):



Types of Server Certificates

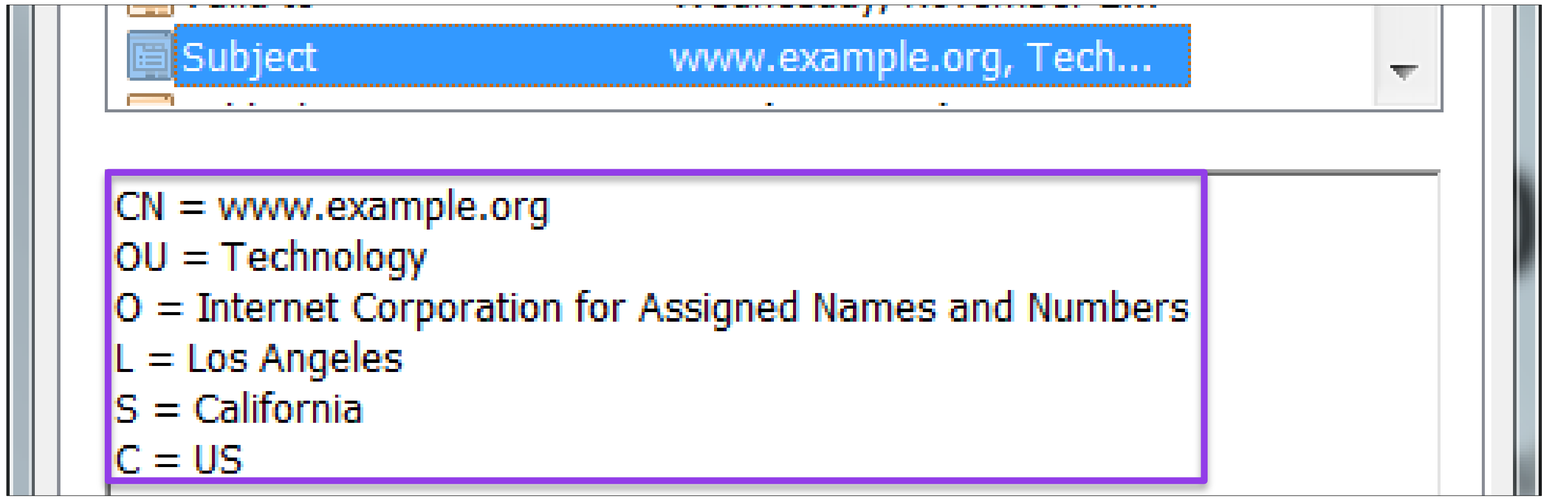
Organization Validated (OV) – Basic identity confirmation through simple vetting, confirmed customer contact using reliable third party data



Types of Server Certificates

Organization Validated (OV)

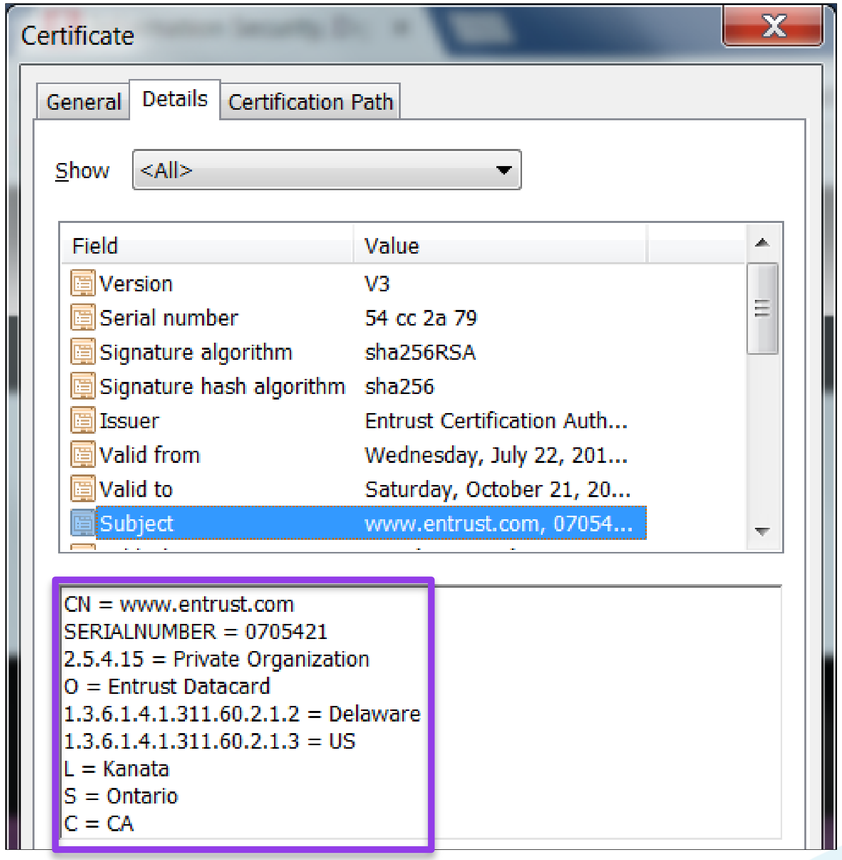
Close Up:



Sample Browser Treatment (Chrome):

Types of Server Certificates

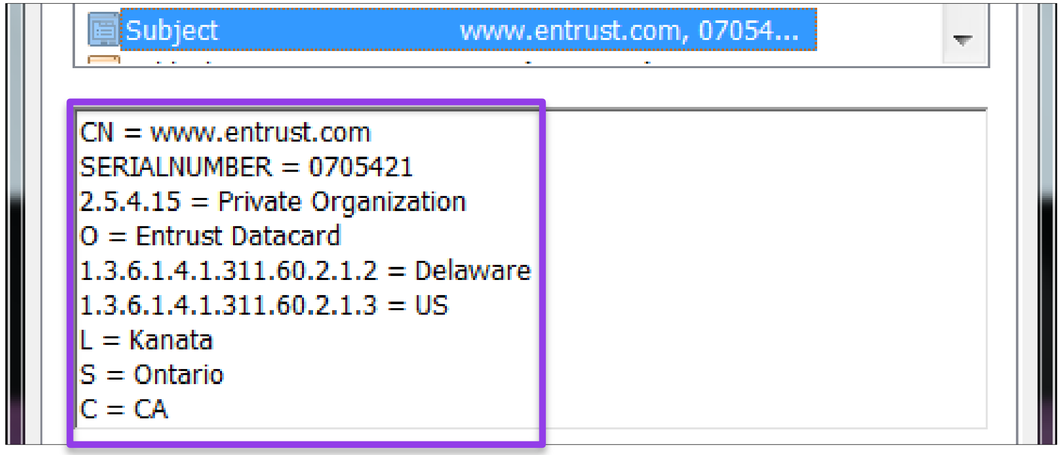
Extended Validation (EV) – Strong identity confirmation through extensive vetting using reliable third party data, and government registries



Types of Server Certificates

Extended Validation (EV)

Close Up:



Sample Browser Treatment (Internet Explorer):

RSA Conference2017

Past and Present Browser UI Security Indicators

Past and Present Browser UI Security Indicators

1995-2001: Organization Validation (OV) only; two UI security states

1	No certificate (http)	= Normal state
2	OV Certificate with identity information - only OV certs in this period – (https)	= Padlock

2001-2007: Domain Validated (DV) added as alternative to OV; still only two security UI states – no differentiation between DV and OV

1	No certificate (http)	= Normal state
2	DV or OV Certificate (DV certs ***without*** identity information – https) (OV certs ***with*** identity information - https)	= Padlock (***no distinction*** between DV and OV)

Past and Present Browser UI Security Indicators

2007-Present: Extended Validation (EV) added as alternative to DV and OV

Four **security UI states,** including "problem" state; still no differentiation between DV and OV

1	Problem site	= Warning state, often with icons such as ⊘ or ⚠
2	No certificate (http)	= Normal state
3	DV or OV Certificate (DV certs ***without*** identity information – https) (OV certs ***with*** identity information - https)	= Padlock (***no distinction*** between DV and OV)
4	EV Certificate (EV – https with strongly confirmed identity information)	= Green padlock and identity information (Org. Name and Jurisdiction) in green bar

RSA Conference 2017

Positive Developments in Encryption

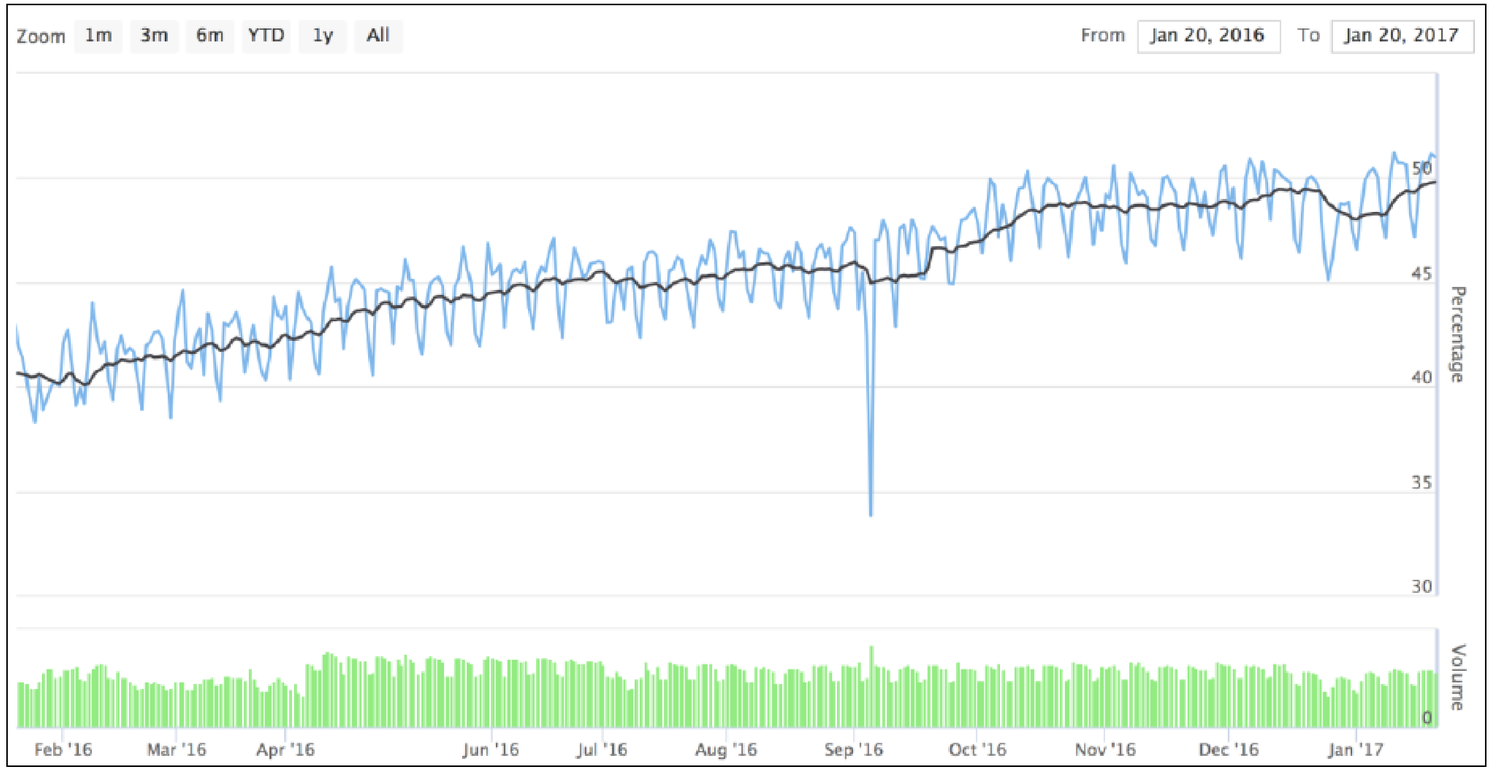
Positive Developments in Encryption

- **Rapid move to encryption** – Web now over 50% encrypted
- **Browsers mandating encryption in stages** – otherwise receive negative browser UI ⚠ – "https://" becoming the new normal
- Encrypted sites receive **higher SEO rankings**
- **Automated certificate issuance and installation** – Boulder, ACME, Certbot – make it easy for small users
- **Free DV certificate services** – Let's Encrypt and others – encourage websites to try it out
- The **PCI Security Standards Council** recommends the **use of OV/EV certs** as part of the Best Practices for Safe E-Commerce

Source: https://www.pcisecuritystandards.org/pdfs/best_practices_securing_ecommerce.pdf

Positive Developments in Encryption

Encryption is increasing rapidly – now over 50%



Source: Firefox Telemetry Data

Positive Developments in Encryption

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

RSA Conference2017

Negative Developments in Encryption

Negative Developments in Encryption

Malware exploits are moving to encryption and are harder to block

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 *** 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 security tools."*

Source: http://www.infosecurity-magazine.com/news/rising-use-of-encryption-gives/

Negative Developments in Encryption

DV certificates are now the default choice for fraudsters – “look-alike” names, anonymity, free, the padlock, no UI warnings:

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

Negative Developments in Encryption

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***."

Source: http://news.netcraft.com/archives/2015/10/12/certificate-authorities-issue-hundreds-of-deceptive-ssl-certificates-to-fraudsters.html

Negative Developments in Encryption

Many browsers no longer do effective revocation checking

CONCLUDING DISCUSSION

"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*."

Source: https://web.stanford.edu/~aschulm/docs/imc15-revocation.pdf

Negative Developments in Encryption

Some CAs no longer do certificate revocation for encrypted malware sites

Let's Encrypt believes 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 in 2015." So Let's Encrypt will not revoke for phishing or fraud.

"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.

Source: https://letsencrypt.org/2015/10/29/phishing-and-malware.html

Negative Developments in Encryption

Users assume all encrypted sites with padlocks are “safe” sites:

“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.**

“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.”

Fraudsters also sprinkle static “padlocks”  all over the page to fool users.

Source: http://www.datamation.com/security/lets-encrypt-the-good-and-the-bad.html

What About Browser Website Filters?

Browser website filters expand, but are not a complete solution for user safety – thousands of bad sites are not included

Microsoft SmartScreen problems: Only protects users in Windows

- Users can't report phishing URLs – must visit bad site first to report, click on button
- SmartScreen filters can be bypassed by fraudster email / click-throughs to bad site

Google Safe Browsing: Only works on Google search results / Google properties

- Privacy issues – cookies, retains browsing records on same device
- Relies on proprietary Google algorithms, not transparent to users

Both SmartScreen and Safe Browsing must be turned on to work

Reactive systems –back to the '90s

Like cops solving a crime *after* it happens – but not *preventing* the crime

Many Bad Sites Missed by Browser Filters

Thousands of Malware / Phishing sites not detected	
SmartScreen	**Safe Browsing**
usbbackup.com/cgi-biin/update.apple-id.com/4bebac1b93b057sjgurnm94a6b06c59b7/login.php 0760mly.com/js/wwwpaypalcom/IrelandPayPal/signing38CountryIE/ieLogIn.html aggelopoulos.com/wp-content/uploads/2008/ 07/ www.paypal.com/beta.entab9387.net/wp-theme/image/img/DHL/tracking.php https://gallery.mailchimp.com/2724801a312bda1123d554199/files/Electronic_Shipping_Document.zip	http://121.134.15.63/www.paypal.com/websc-login.php http://alfssp.net/www.confirm.paypal.com/websc-login.php http://aquaseryis.marag.pl/wp-includes/random_compat/apple.co.uk/ https://gallery.mailchimp.com/2724801a312bda1123d554199/files/Electronic_Shipping_Document.zip

[URLs modified for safety]
Source: Comodo Valkyrie malware analysis system
More phishing links: http://cdn.download.comodo.com/intelligence/ctrl-06-02-url.txt
More malware file links: http://cdn.download.comodo.com/intelligence/ctrl-06-01-url.txt

What more can be done?

So what more can we do to protect users in 100% encrypted environment…?

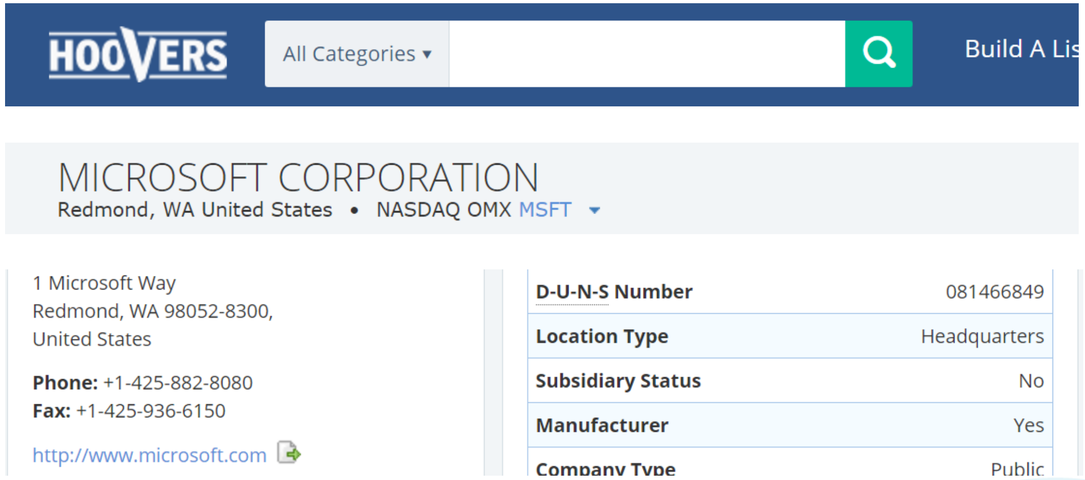
RSA Conference2017

Using Identity in Certificates as a Proxy for User Safety

Confirming Identity – How It's Done

Organization Vetting (OV)

- **Find** the customer in a reliable third party database, such as Dun & Bradstreet or Hoover's
- **Call** the customer representative through a number found on the third party data source, confirm order is legitimate: *+1-425-882-8080* for Microsoft
- **Confirm** domain ownership or control (using CA/Browser Forum Methods)



Confirming Identity – How It's Done

Extended Validation Vetting (EV) – All that and more:

- Confirm active status of corporation with government agency
- Check authority of customer rep with company HR Department
- Check against blacklists, prohibited lists, etc.

Secretary of State
Kim Wyman

Corporations

MICROSOFT CORPORATION

View Additional Information »

Purchase Documents for this Corporation »

UBI Number	600413485
Category	REG
Profit/Nonprofit	Profit
Active/Inactive	Active

Registered Agent Information

Agent Name	CORPORATION SERVICE COMPANY
Address	300 DESCHUTES WAY SW STE 304
City	TUMWATER
State	WA
ZIP	985017719

What's the Problem With Current Browser UIs?

- No consistency among browser UIs as to four states: unencrypted, DV, OV, and EV
- Individual browsers frequently change their own UI, users can't keep up
- Adding array of other warnings to UI (minor problems, major problems) that the average user doesn't understand
- Most mobile devices don't even show any symbol for encryption
- As a result, users are confused about how to read browser UIs

TAKE A LOOK…

What Does This Mean? Universal - “STOP!”

What if “Stop” Signs Were Always Changing?

That’s what browser UI security indicators have done – user confusion!

What Does Any of This Mean? What a Mess!

Browser	HTTP	HTTPS	EV
Chrome 48 Win	www.exam	https://www	Symantec Co
Edge 20 Win	example.com	example.	Symantec Co
Firefox 44 Win	www.example	https://www.e	Symantec Corpo
Safari 9 Mac	example.com	example.com	Symantec Cor
Chrome 48 And	www.examp	https://v	https://v
Opera Mini 14 And	www.example	www.exam	www.syma
UC Mini 10 And	Example D	Example D	Endpoint, C
UC Browser 2 iOS	Example Do.	Example Do.	Endpoint, C.
Safari 9 iOS	example.com	example.c	Symantec

Source: Rethinking Connection Security Indicators, https://www.usenix.org/system/files/conference/soups2016/soups2016-paper-porter-felt.pdf

More Examples of Confusing Browser UIs

Browser UI Security Indicator:	HTTP only (no certificate)	DV certificate	OV certificate	EV certificate
Chrome 55 (Windows)	www.example.com	https://casecurity.org	https://www.example	Trustwave Holdings, Inc. [US] | https://www.trust
Chrome 48 (Android)	www.example.com	https://example.com	https://www.example	https://www.globalsign.com/en/
Edge 20 (Windows)	example.com	casecurity.org	example.com	GoDaddy INC. [US] godaddy.com
Firefox 50 (Windows)	www.example.com	https://casecurity	https://www.exar	COMODO CA Limited (GB) | https://crt.sh
Safari 9 (Mac)	example.com	casecurity.org	example.com	GMO GlobalSign Inc
Safari 10 (iOS)	example.com	casecurity.org	example.com	GMO GlobalSign Inc
OperaMini 14 (Android)	www.example.com	casecurity.org	www.example.con	www.Entrust.com
UC Mini 10 (Android)	Example Domain	CA Security Council	Example Domain	SSL & Digital Certificates by GlobalSign
UC Browser 10.8.7.903 (iOS)	example.com	CA Security Council	example.com	SSL Digital Certificate Authority

Source: CA Security Council (CASC)

Plus, What Do All These Warnings Mean?

Browser UI Security Indicator:	HTTPS Minor Error	HTTPS Major Error
Chrome 55 (Windows)	https://mixed.example.com	~~https~~://wrong.host.badssl.com
Chrome 48 (Android)	https://mixed.badssl.com	~~https~~://www.example.com
Edge 20 (Windows)	mixed.badssl.com	wrong.host.badssl.com
Firefox 50 (Windows)	https://mixed.badssl.com	https://wrong.host.badssl.com
Safari 9 (Mac)	mixed.badssl.com	wrong.host.badssl.com
Safari 10 (iOS)	mixed.badssl.com	wrong.host.badssl.com
OperaMini 14 (Android)	mixed.badssl.com	wrong.host.badssl.com
UC Mini 10 (Android)	mixed.badssl.com	mixed.badssl.com
UC Browser 10.8.7.903 (iOS)	mixed.badssl.com	wrong.host.badssl.com

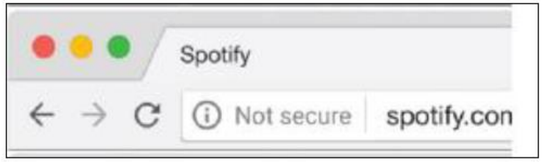
Source: CA Security Council (CASC)

Help Is On The Way! …Or is it?

June 2016 Google UI paper proposed standardizing around only three security states – but basically a **binary, two-state** "secure/not secure" UI. Plus, EV UI may be **disappearing**:

1. Security Indicator for HTTPS – "***Secure***"

2. Security Indicator for HTTP only - no encryption – "***Not secure***"



3. Security Indicator for Invalid HTTPS - encrypted but with mistakes "***Not secure***"

Google Binary UI Proposal

Good:

1. Security Indicator for HTTPS – "***Secure***"

No more EV?
DV, OV, EV all the same?

Bad:

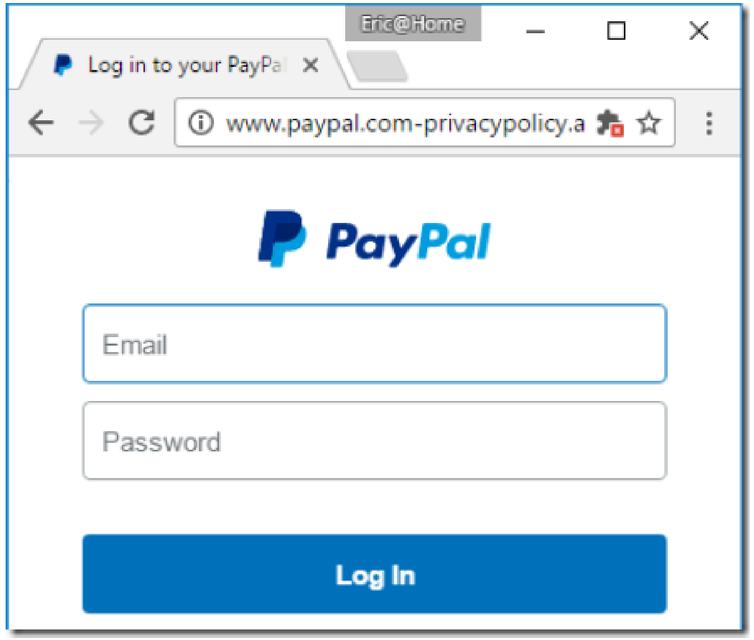
2. Security Indicator for HTTP only - no encryption – "***Not secure***"

3. Security Indicator for Invalid HTTPS - encrypted but with mistakes "***Not secure***"

Here's What This Can Mean

Phishing site: paypal.com.summary-spport.com

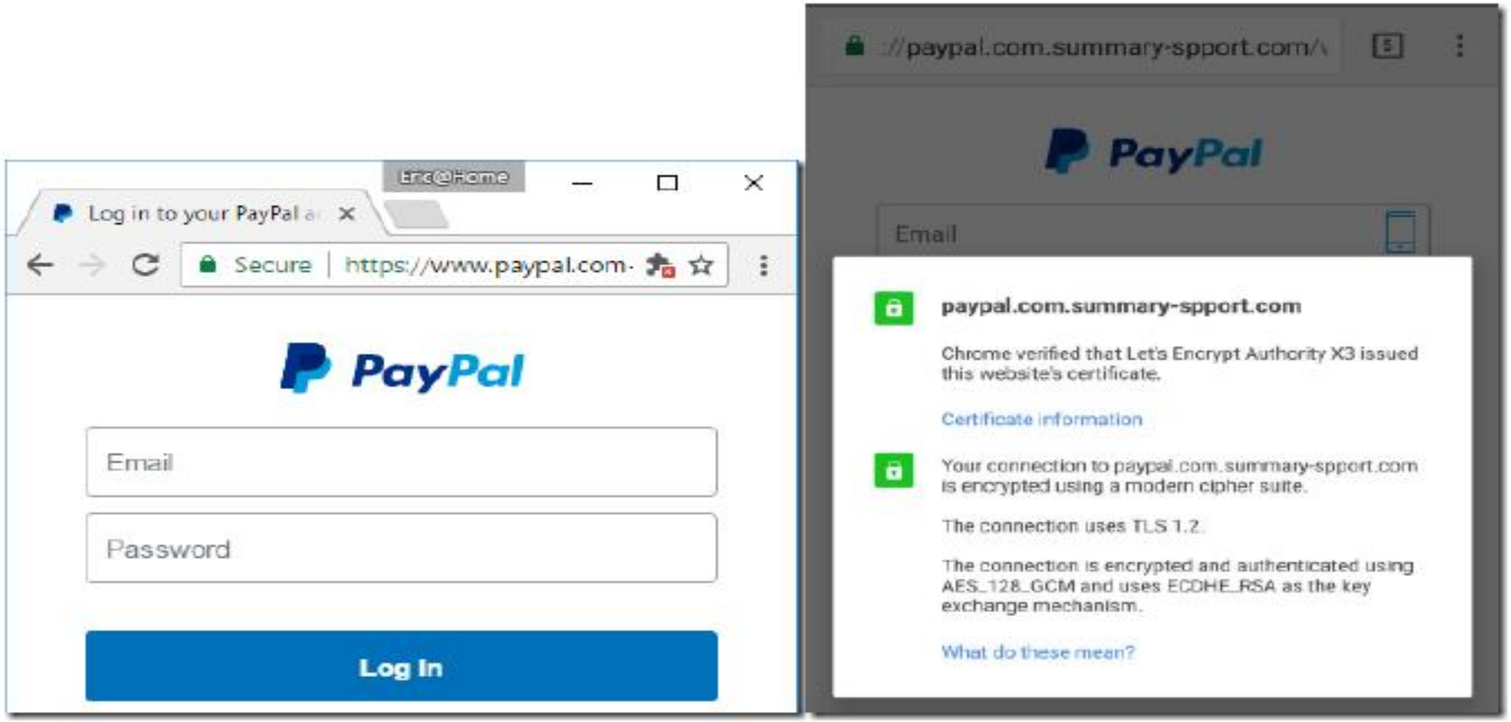
Here's how it looks as an *http* site today – just a gray circle-i:



Soon, Chrome will treat *http* sites as *"Not Secure"*: Not secure

Phishers will move to DV certs for “Secure” UI

Phishing site: paypal.com.summary-spport.com gets anonymous, free DV cert:

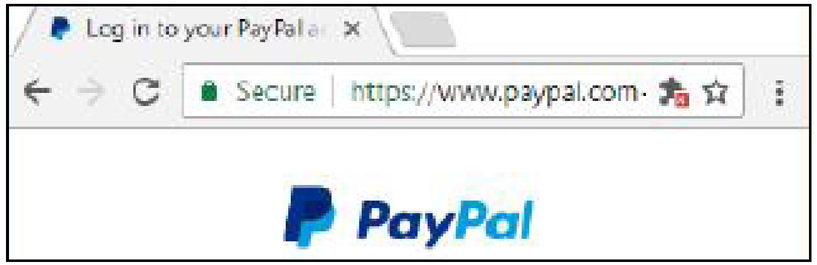


Chrome gives “Secure” *https* browser UI to phishing site: 

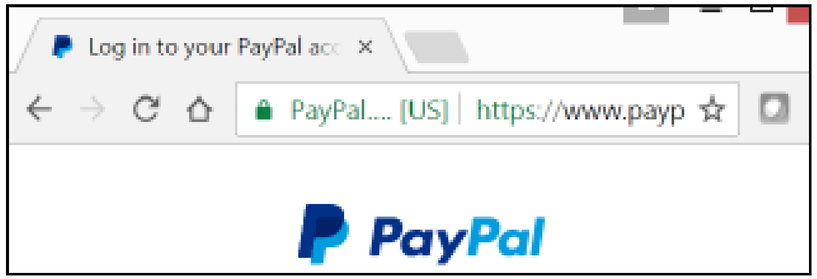
Is This the Future?

If EV green bar display is ***lost*** in Chrome, and *real* and *phishing* PayPal Login pages look the same ("Secure") – *Can't tell the difference!*

Fake PayPal login page today (DV)
www.paypal.com.summary-spport.com



Real PayPal login page today (EV)
www.paypal.com/signin



Real PayPal login page in the future (if EV certs downgraded, all UIs the same – DV, OV, and EV)
www.paypal.com/signin

2016 Study – *https* alone no longer effective for anti-phishing, EV indicators can be improved

"In the past, HTTPS was viewed as a sign of website trustworthiness; getting a valid HTTPS certificate was too difficult for typical phishing websites. *** 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. ***

"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. *** Improving EV indicators are out of scope for our current work."

Source: Rethinking Connection Security Indicators, https://www.usenix.org/system/files/conference/soups2016/soups2016-paper-porter-felt.pdf

Chain of Logic

- Browsers are pushing website owners to 100% encryption (good)
- Fraudsters are rushing to free DV certs to hide (bad)
- DV certs are free, allow anonymity, no identity, no 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; EV may be downgraded to same level as DV and OV by Chrome in future release
- Conclusion: We are wasting valuable identity information already inside OV and EV certs – should use as a proxy for user safety

Let's Use the Data We Already Have

There is so much *identity data* in certificates today – but most of it's hidden

Why aren't we using identity data to block phishing and malware sites?

2016 Data

Type	Number (000s)	Percent	Combined
DV	7,503	75%	
OV	2,353	24%	**25%**
EV	243	1%	

Source: Frost and Sullivan

RSA Conference2017

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

Five Principles of TLS Certificate Identity

First, adopt the Five Principles of TLS Certificate Identity:

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.

Here's Who Has Endorsed the Five Principles

Current endorsers of the Five Principles of TLS Certificate Identity and adoption of a new "Universal" browser UI:

- Entrust Datacard
- COMODO
- digicert
- GlobalSign GMO INTERNET GROUP
- GoDaddy™
- Symantec
- Trustwave
- CA Security COUNCIL

More CA endorsers to come…

Do website owners care about identity? *You bet they do!* (No one asked them before…)

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 endorse these Website Identity Principles:

Website owners who support Website Identity Principles

ESTĒE LAUDER
Teleperformance
INTERNATIONAL MONETARY FUND
GameStop
UNITED STATES POSTAL SERVICE
AMERICAN EXPRESS
WESTERN UNION
viacom
Western Digital
MERCK
SANOFI
macy's
MICHELIN A better way forward
ups
WARNER BROS. PICTURES
COMCAST
NYSE
PEARSON Education
BRINKS
ETS
NETGEAR
PUBLICIS GROUPE
ADT Security Services
at&t
DTE Energy
IDT
GOODYEAR
Johnson & Johnson
HBO
E*TRADE
Elavon
UnitedHealthcare
THE WORLD BANK IBRD • IDA | WORLD BANK GROUP
jetBlue AIRWAYS
Time Inc.

Source: Comodo and Entrust Datacard

Plus many more enterprise endorsers!

Sign up to support the Website Identity Principles at CASC site: casecurity.org/identity

Adopt a "Universal" UI for all Browsers

Here is a proposal that would work for desktop and mobile environments. This is just a *starting point for discussion*…

Universal Browser UI – Ideal for Desktop and Mobile	
HTTPS EV	Citigroup Inc.
HTTPS OV	bing.com
HTTPS DV & Minor Security Issues	example.com
HTTP & Broken HTTPS	Not secure

Design by: Chris Bailey

Obstacles and Responses to "Universal" UI

- "Users don't understand the difference among DV, OV, and EV"

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

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

  Response: CAs standardized OV vetting in 2012, and can strengthen further

- "We browsers will decide safety for our users – maybe just a binary UI"

  Google approach – but totally wastes available identity information in certs

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

  Response: announce a year ahead – customers will migrate to OV to get the better UI

User Education will be Based on Cert Guidelines

To help develop user education, start by defining when to use each type of certificate:

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

How Do We Educate Users on the New UI?

Here's the 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 ten years ago – we can train them again with new, common UI security indicators

RSA Conference2017

Next Steps

Next Steps for User Security

- Browsers should **collaborate** and adopt a common "Universal" UI
- Browsers should announce a **transition date** to new Universal UI
  - 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
- 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*

Summary

- Fraudsters are moving to DV certificates
- Fraudsters hate identity – they avoid OV and EV certificates
- Therefore, OV and EV certs (25% of sites) represent much *safer* sites for users – prevent crime
- On this basis, OV and EV certs deserve their own distinct browser UIs for user safety
- DON'T eliminate EV UI, DON'T create binary UI of "secure" vs. "not secure"- that hides identity
- Browsers should work together to create a common Universal UI
- All should work together to educate users on the new Universal UI

RSA Conference2017

Thank you! Questions?

Download White Paper *"Use of Identity in SSL-TLS Certs for User Safety"* and sign petition at: casecurity.org/identity

The First Draft of a "Universal" UI

Universal Browser UI – Ideal for Desktop and Mobile	
HTTPS EV	Citigroup Inc.
HTTPS OV	bing.com
HTTPS DV & Minor Security Issues	example.com
HTTP & Broken HTTPS	Not secure

Design by: Chris Bailey