

Creating a more intuitive method of displaying secure sites to Internet users

Chris Bailey, VP Trust Services

What's the purpose of the Forum?

Bylaws 1.1 - Purpose of the Forum

“Members of the CA/Browser Forum have worked closely together in defining the guidelines and means of implementation for best practices as a way of

- [1] providing a heightened security for Internet transactions and
- **[2] creating a more intuitive method of displaying secure sites to Internet users.”**

We've done a lot on #1, but nothing on #2



“Secure” Site Indicators

Browsers use security indicators to communicate connection security states, website trustworthiness, or a combination of the two¹

1) Source: “Rethinking Connection Security Indicators” Authors: Adrienne Porter Felt, Robert W. Reeder, Alex Ainslie, Helen Harris, and Max Walker, Google; Christopher Thompson, University of California, Berkeley; Mustafa Emre Acer, Elisabeth Morant, and Sunny Consolvo, Google



“Intuitive”

- Defined as - Using or based on what one feels to be true even without conscious reasoning; instinctive¹
- Or - (chiefly of computer software) easy to use and understand.¹
- Design does not become intuitive by magic. When we experience a design as intuitive, it's because we have encountered something like it before.²
- This means some type of Repetition...

1) Source: Google.com lookup “Intuitive”

2) Source: <https://www.interaction-design.org/literature/topics/intuitive-design>



“Repetition”

- The action of repeating something that has already been said or written¹
- One way to accomplish repetition across environments so users can understand it intuitively is to have standards

1) Source: Google.com lookup “Repetition”



“Standards”



















- An idea or thing used as a measure, norm, or model in comparative evaluations¹

1) Source: Google.com lookup “Standards”



Secure Site Indicators Have Never Been Standardized

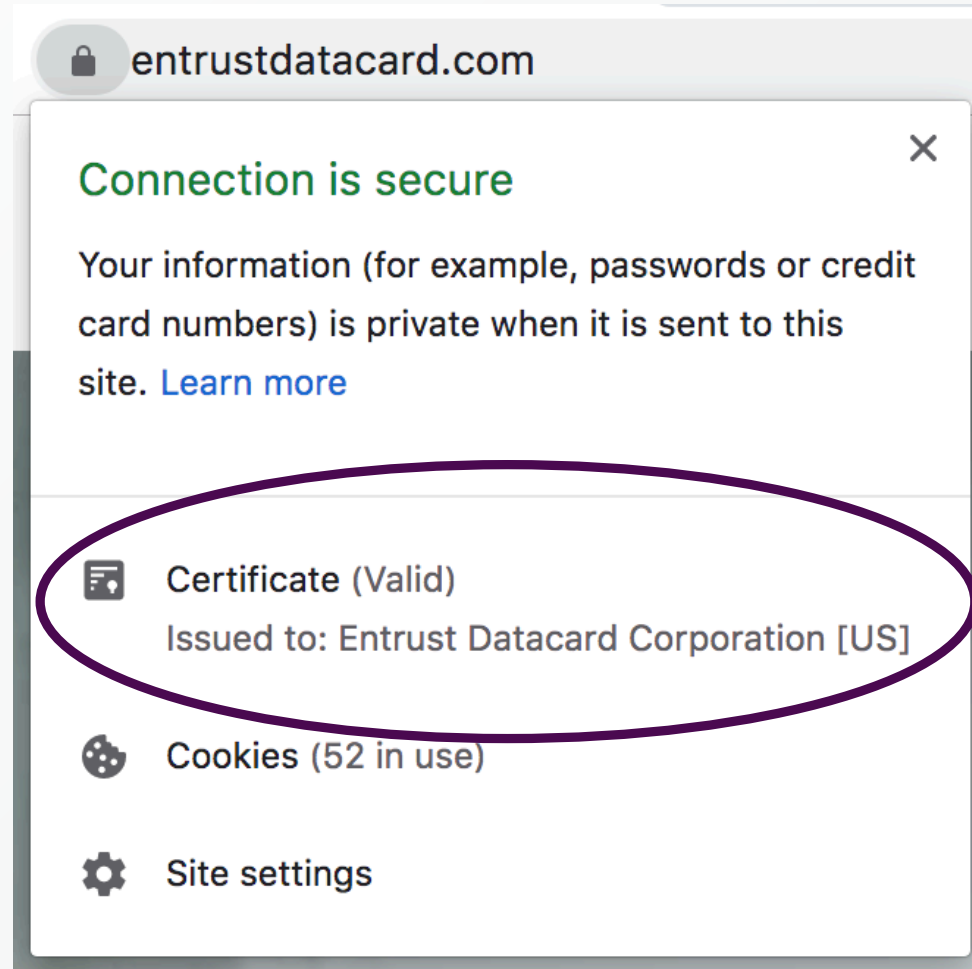
There have been several browser changes since this figure from 2016.

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

Source: "Rethinking Connection Security Indicators" Authors: Adrienne Porter Felt, Robert W. Reeder, Alex Ainslie, Helen Harris, and Max Walker, Google; Christopher Thompson, University of California, Berkeley; Mustafa Emre Acer, Elisabeth Morant, and Sunny Consolvo, Google



Including the most recent changes to the EV UI showing EV in Chrome / Firefox



This is not an intuitive way to display secure sites with EV to Internet users

1. No EV information in the URL Bar and no standardized way to show EV information in the URL Bar
2. No intuitive or standard way to look up EV identity data



One way to make things intuitive is to standardize

The STOP sign was Internationally standardized in 1968 via the Vienna Convention on Road Signs and Signals – current octagonal red around the world.

Today the stop sign is so intuitive that most children know what a stop sign means



Some Potential Design Constraints for Security Indicators

1. The indicators need to scale down for small devices. Icons should not rely on small decorations that become illegible when small. We can optionally use text, but there will not always be space to display it.
2. The icon shape alone — without color — needs to communicate the level of risk to meet accessibility needs. 8% of men are colorblind¹, and many others have vision impairments.
3. The indicator's meaning needs to be taught with words when possible. Millions of new Internet users have recently come online via smartphones without learning “standard” iconography from desktop browsers.²
4. Others ?

1) L. T. Sharpe, A. Stockman, H. Jagle, and J. Nathans. Opsin genes, cone photopigments, color vision and color blindness. In K. R. Gegenfurtner and L. T. Sharpe, editors, *Color Vision: From Genes to Perception*. Cambridge University Press, 1999

2) Source: “Rethinking Connection Security Indicators” Authors: Adrienne Porter Felt, Robert W. Reeder, Alex Ainslie, Helen Harris, and Max Walker, Google; Christopher Thompson, University of California, Berkeley; Mustafa Emre Acer, Elisabeth Morant, and Sunny Consolvo, Google



Other UI Design Considerations

- Once common elements of a UI/UX are chosen, browsers should not re-use the same elements for other purposes
- Design a quick way to see more data with a single click?
- Develop common user training elements



- In the past, many browsers implemented the EV UI similar to this:



- And DV/OV encrypted sites like this:



- Mobile was just emerging which helped cause a “split” in the mobile and desktop version of the EV UI in the URL bar.

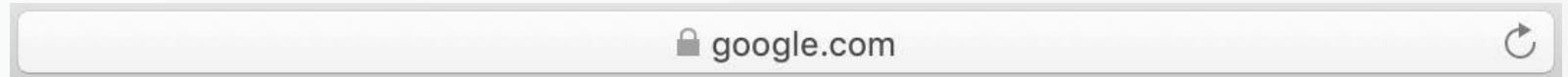


Apple takes a more minimalist approach to its EV UI

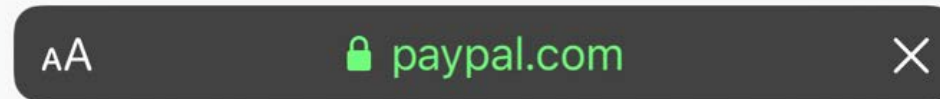
macOS Mojave (Light Mode) – Safari encrypted with Extended Validation



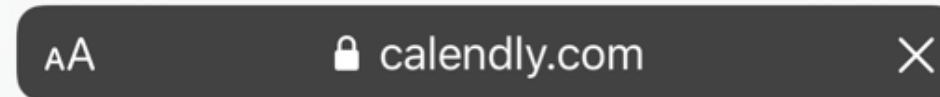
macOS Mojave (Light Mode) – Safari encrypted without Extended Validation



iOS 13x (Dark Mode) – Safari encrypted with Extended Validation



iOS 13x (Dark Mode) – Safari encrypted without Extended Validation



iOS 13x (Dark Mode) – Safari encrypted without SSL / TLS



*Users can choose between Dark Mode or Light Mode (default) for the appearance of their OS UI



Pros and Cons to the Apple Approach

Pros

- Very easy to implement
- Fits on multiple screen sizes

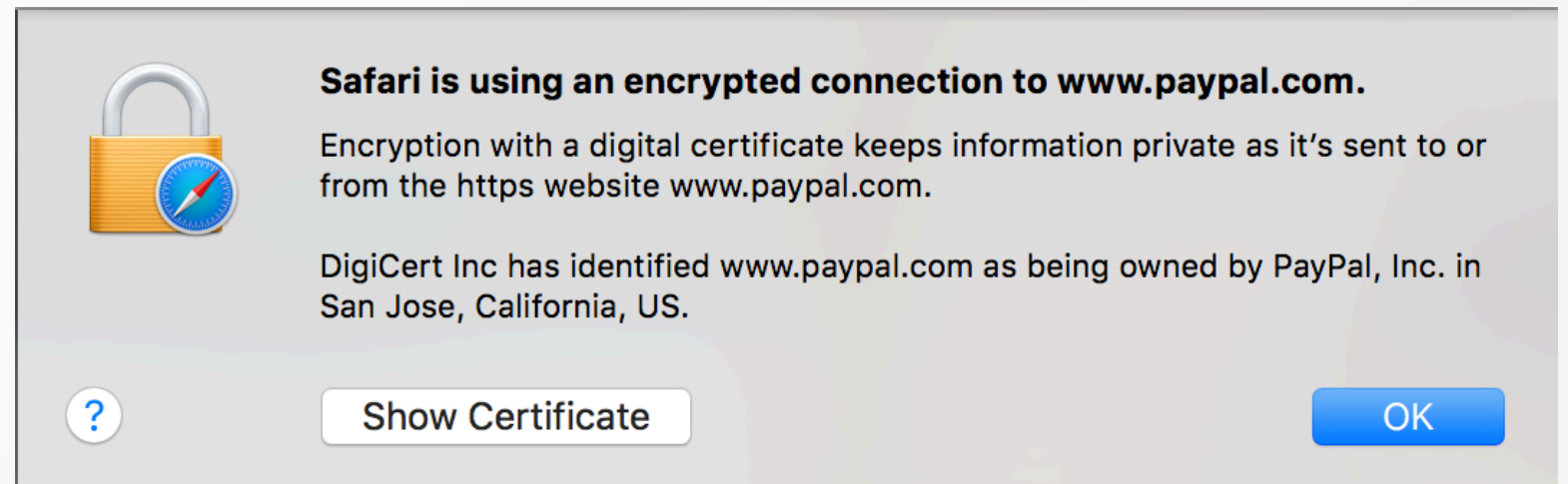
Cons

- Color Blindness still an issue? Potential solutions (add symbol, bold text, and / or add more textual data, etc...)
- Organization Identity is removed from the URL
- Potential issue – could use a single EV certificate to secure multiple non-related sites - the Hosting Problem



How do you find more data about the site in Safari?

- When you click on the lock symbol in MacOS





- Unfortunately, this data is not available in iOS when you click on the lock symbol



This is the way
Firefox presents EV
identity data –
unfortunately you
have to click twice
to see the full EV
data


Site Information for www.paypal.com

 **Connection secure**
Certificate issued to: PayPal, Inc. >

 **Permissions**
You have not granted this site any special permissions.

Clear Cookies and Site Data...

< **Connection Security for www.paypal.com**

 **You are securely connected to this site.**

Certificate issued to:
PayPal, Inc.
San Jose
California, US
Verified by: DigiCert Inc

More Information



How does the Forum “*create a more intuitive method of displaying secure sites to Internet users*”?

- Look for common UI elements that work across all platforms – desktop and mobile
- Develop a list of common UI element recommendations
- Review / modify over time with experience

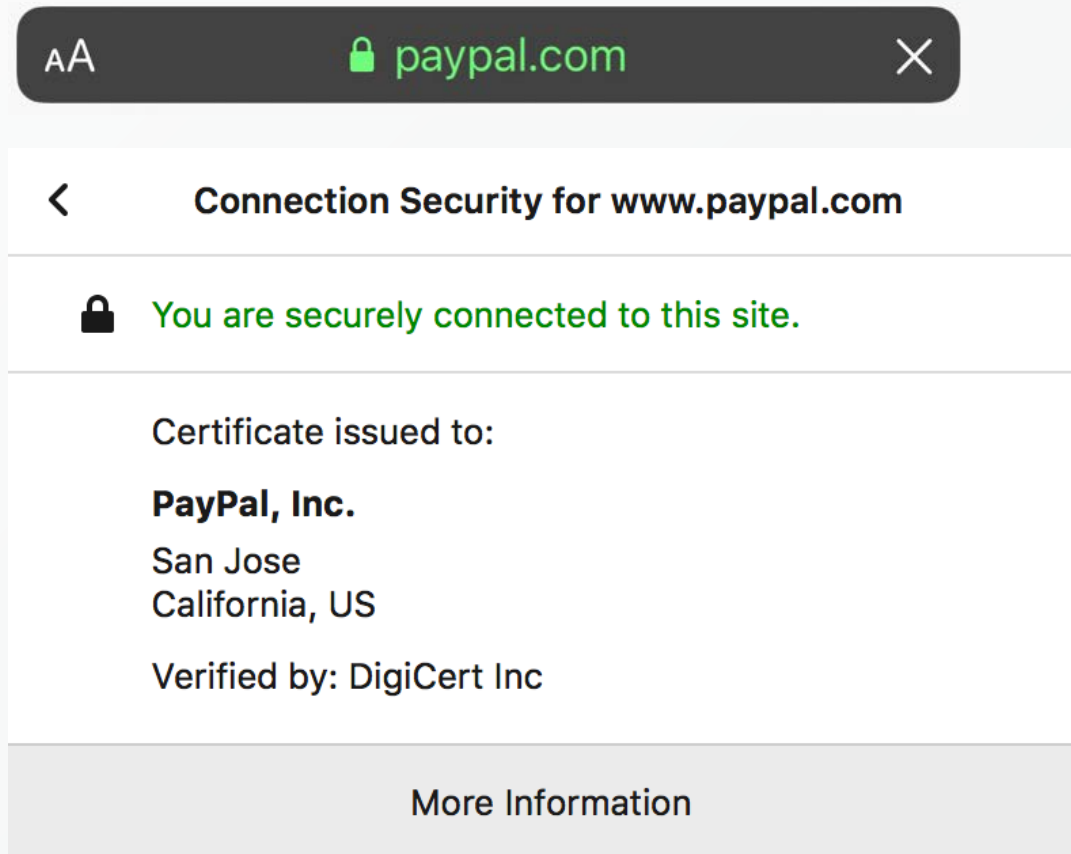


Next steps?

- Create a “straw person” set of recommended browser/app UX/UI elements (to generate the most response, pro and con)
- Apple has solved a lot of problems, maybe we begin by leveraging their UI scheme in the URL Bar for Desktop and Mobile (green lock and green FQDN / DN)? Plus, use the “click on the lock” for the full identity data in a structured format similar to the “second click” in Firefox.



Example



Next steps?

- Issue a call for participation:
 - Discussion list
 - Teleconferences
 - F2F meetings
- What else?



Who should be involved in this effort?

- This will be a set of voluntary, industry-recommended common UI/UX elements
 - Browsers and CAs (including their UI/UX design experts)
 - Outside experts including academics
 - Site Owners
 - Interested governments
 - Who else?



Wrap Up

- The Forum has done great work in the past by consensus among browsers and CAs (BRs, NetSec, EVGL), raising the bar for the industry and improving security for everyone on a collaborative basis
- This is an important project and can truly help users
- Let's get started!
- **Questions / comments?**





Entrust Datacard™

Trusted Identities | Secure Transactions