Update on London Protocol

Kirk Hall

June 13, 2019

Entrust Datacard™

RECAP OF LONDON PROTOCOL

- Named after London CABF meeting in June where Protocol announced
- Project of CA Security Council (CASC)
- Seven current participants: Buypass, D-Trust, Entrust Datacard, GlobalSign, GoDaddy, Sectigo, SecureTrust
- Any CA can participate – not just CASC members. Sign up now!
  - chris.bailey@entrust.com

- **Objective of London Protocol**: Reinforces the distinction between *Identity Websites* (OV and EV) by making them *even more secure* for users than websites encrypted by DV (domain validated) certificates.

Our philosophy: User security is best when done *in depth*, with multiple layers and parties involved (browsers, CAs, security applications/anti-phishing services) each providing their own contribution to fill the gaps in user security provided by others. No one security method or provider covers all user threats 100% of the time.

OBJECTIVE OF LONDON PROTOCOL:

The London Protocol is not any one thing, but a framework that tests new ideas to improve identity assurance and user security, and then share the results with the larger community.

Today we are working on **four services**, but there could be others as well:

1. Anti-phishing solution
2. Flag list system
3. Identity collision system
4. Transparency (as to data sources used for EV validation of SubjectDN data) – *in development*

This information can then be *utilized* by:

- *Users / machines* as to the type of website they are visiting
- This information is leveraged today by *antiphishing engines* in their security algorithms
- Other – such as browser UIs

LONDON PROTOCOL PART 1 – ANTI-PHISHING SOLUTION

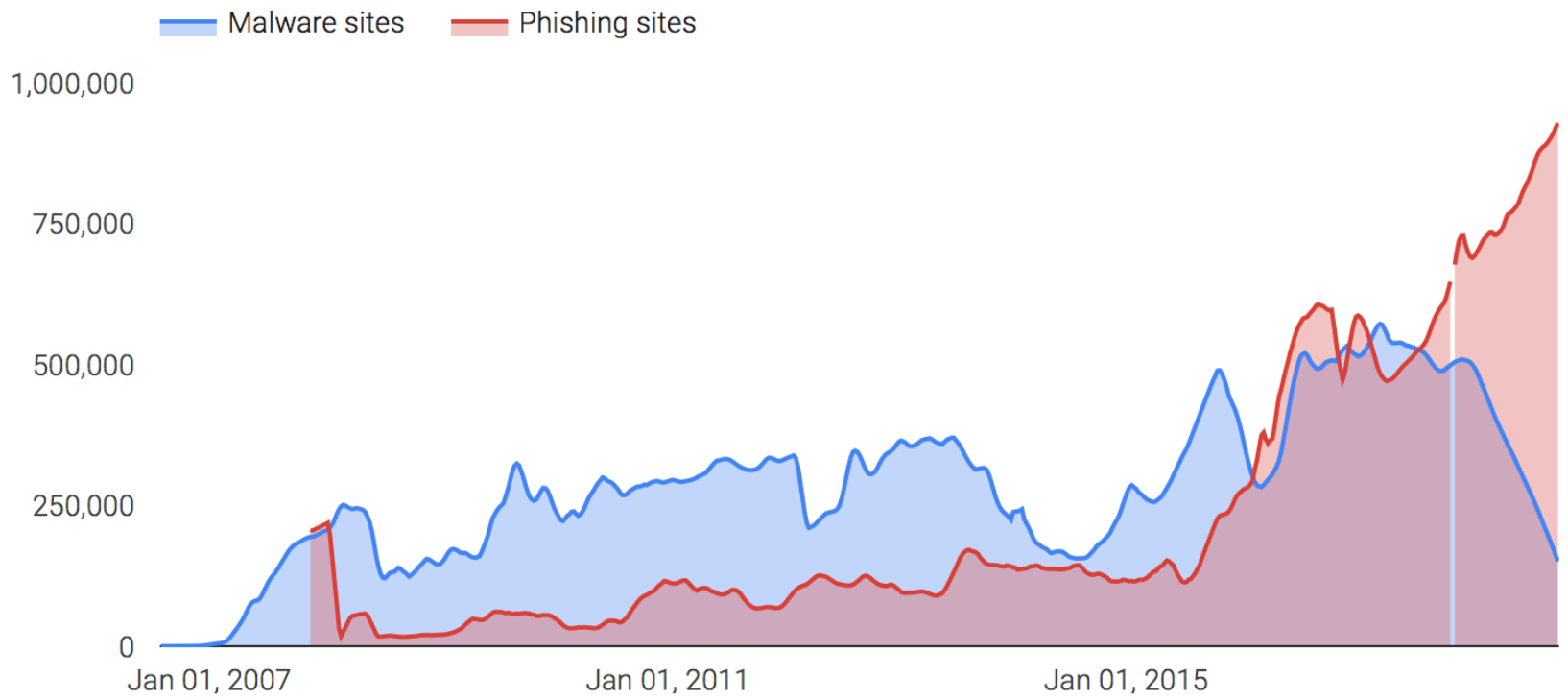
Objective - minimize the possibility of phishing activity on websites encrypted by OV (organization validated) and EV (extended validation) certificates. These sites are already safer for users (much less phishing than DV sites), and we want to make them as close to absolutely safe as possible

It may be possible for CAs to extend to DV certs in the future if warranted – *but*:

- Many DV sites are actually phishing sites, so notice about phishing content on their sites from issuing CA won't actually do anything
- CA may not have good contact information for the DV customer (other than an email address)
- Some CAs who issue DV certs don't even have an email address to reach the customer – no points of contact at all!

SITES DEEMED DANGEROUS BY GSB – OCTOBER 2018 (GETTING BAD)

START 5/21/2006 END 10/7/2018

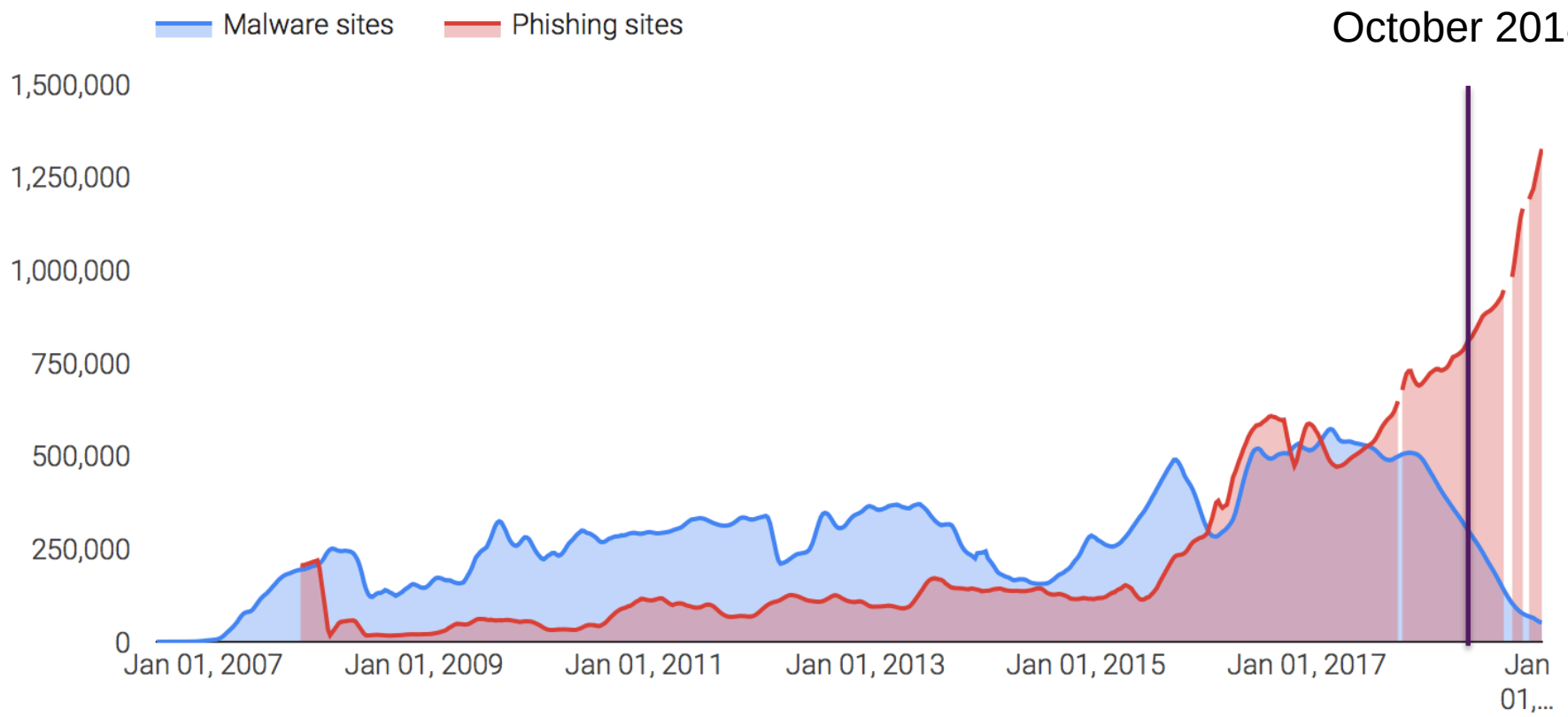


SELECT DATASET NUMBER OF SITES DEEMED DANGEROUS BY SAFE BROWSING

Source: https://transparencyreport.google.com/safe-browsing/overview

SITES DEEMED DANGEROUS BY GSB – MARCH 2018 (GETTING *WORSE!*)

START 5/21/2006 END 3/2/2019



October 2018

Last date that Google reports is March 2, 2019, so no new statistics yet

SELECT DATASET NUMBER OF SITES DEEMED DANGEROUS BY SAFE BROWSING

EFFICACY OF BROWSER FILTERS

Browser Filters are great – but they don't eliminate all phishing sites. They are not a complete solution for user security.

Time to Protect	Microsoft Edge	Google Chrome	Mozilla Firefox
0-Hour	89.0%	79.0%	77.0%
1 day	89.0%	79.0%	77.0%
2 days	97.0%	95.0%	95.0%
3 days	98.0%	96.0%	96.0%
4 days	98.0%	96.0%	96.0%
5 days	98.0%	96.0%	96.0%
6 days	98.0%	96.0%	96.0%
7 days	98.0%	96.0%	96.0%
Protection Score	93.6%	87.9%	87.0%

https://research.nsslabs.com/library/endpoint-security/web-browser-security/wbs-2018-comparative-report-protection-against-phishing/

INCIDENCE OF ENCRYPTED PHISHING BY CERT TYPE

- This table shows breakdown of encrypted phishing sites by certificate type for the month of **September 2018**

Certificate Type	Entrust/Comodo/GSB Dataset		The Internet	
	Phishing Sites in Sample (1)	Percent of Total Phishing Sites in Our Sample	Total Internet Certificate Population (1)	Percent of Total Cert Population
EV	0	0.00%	211,242	0.48%
OV	61	1.61%	2,485,895	5.69%
DV	3716	98.39%	41,047,236	93.83%
Total	3777	100.00%	43,744,293	100.00%

(1) Based on 30 days of phishing sites in September 2018 with SSL / TLS – Source Phishbank
(2) Based on Netcraft valid certificate population by certificate type as of September 2018.

INCIDENCE OF ENCRYPTED PHISHING BY CERT TYPE

- This table shows breakdown of encrypted phishing sites by certificate type for the month of **February 2019**

Certificate Type	Entrust/Comodo/GSB Dataset		The Internet	
	Phishing Sites in Sample (1)	Percent of Total Phishing Sites in Our Sample	Total Internet Certificate Population (1)	Percent of Total Cert Population
EV	0	0.00%	215,298	0.38%
OV	145	4.15%	7,591,949	13.52%
DV	3349	95.85%	48,319,412	86.08%
Total	3494	100.00%	56,126,659	100.00%

(1) Based on 30 days of phishing sites in February 2019 with SSL / TLS – Source Phishbank
(2) Based on Netcraft valid certificate population by certificate type as of February 2019.

INCIDENCE OF ENCRYPTED PHISHING BY CERT TYPE

- This table shows breakdown of encrypted phishing sites by certificate type for the month of **May 2019**

Certificate Type	Entrust/Comodo/GSB Dataset		The Internet	
	Phishing Sites in Sample (1)	Percent of Total Phishing Sites in Our Sample	Total Internet Certificate Population (1)	Percent of Total Cert Population
EV	0	0.00%	216,903	0.35%
OV	1,128	9.5%	10,181,156	16.56%
DV	10,765	90.5%	51,083,756	83.09%
Total	11,893	100.00%	61,481,815	100.00%

(1) Based on 30 days of phishing sites in May 2019 with SSL / TLS – Source Phishbank
(2) Based on Netcraft valid certificate population by certificate type as of May 2019.

INCREASE IN OV PHISHING

Almost all these OV phishing sites are issued to organizations that do not control the content of sites in the OV cert, e.g. hosters. For example: **995 out of 1,128** of these phishing sites (**88%**) using OV are issued off the "CloudFlare Inc ECC CA-2" issuing CA to the Subject Organization = “Cloudflare Inc”

After talking with a few CAs it seems that there is a philosophy is that OV can be issued to *either* the content owner of the site *or* the operator. This philosophy is not shared by all CAs, but this is not a BR violation. The position is that “OV for shared certs is better than a DV certificate because at least an end user has a point of contact if there is an issue.” (Does Cloudflare actually *respond* to any user complaints?) Of course, the other side of the argument is that an end consumer could be confused if this OV data is relied upon as it relates to the site’s content.

Should we address this issue in the Forum?

POTENTIAL OPTIONS TO ADDRESS THIS OV SHARED CERT ISSUE

1. Ignore this issue
2. Match the site content with the organization identity in the certificate? How?
   a) Self-declaration upfront? - Make the requestor declare if they are controlling the webpage content or not, we could flag in certificate, and / or
   b) Require Active or Passive Monitoring by the cert holder (Subscriber) and/or the issuing CA? – **TBD**

METHODOLOGY FOR PHISHING DETECTION

1. The Phishing Detection Service currently relies on phishing data feeds from the following sources:

   OpenPhish, PhishTank, ADMINUSLabs, Blueliv, Anti-Phishing Working Group (APWG), Aslab – Others may be added.

Ready to add other lists. Can we get a list of phishing data directly from

Microsoft, Google, Others – PhishLabs?

2. Confirms suspect URL against Google Safe Browsing (GSB) – so no disagreement that it is a phishing site

We would like to include lists that have a high accuracy rate

3. Attempts to collect screenshots, certificate data, and other statistics to share with issuing CA

Looking to include confirmed phishing, plus other lists, into a flag list system. – This service is being worked on by GoDaddy

WHAT HAPPENS AFTER A CUSTOMER PHISHING SITE IS DETECTED AND CONFIRMED?

- **Step 1:** Participating CAs are notified when customer OV or EV site using their cert is flagged for phishing
- **Step 2:** Issuing CA contacts customer and provides details - URL(s) of phishing content, screen shots, nature of phishing content. If site is using a shared certificate with multiple SANs or independent pages, the customer is told which SANs or pages were flagged for phishing.
- **Step 3:** CA works with customer to help remove the phishing content, how to protect site. If customer will not remediate, CA can consider other steps, even to revocation – each CA decides.
- **Step 4:** Service continues to monitor a phishing website for 30 days (and send notices to CA) until the CA clears the website's status on the phishing list.

SUMMARY – LONDON PROTOCOL PART 1 – ANTI-PHISHING SOLUTION

We think this is the **first** *process* by which website Owners are **proactively** *notified directly* by their Certification Authorities that their sites have been compromised with phishing content, and assisted with recommendations for how to remove phishing content and strengthen site.

This is monitored throughout the entire lifetime of the certificate.

The customers that we have contacted so far have been *very grateful* for our outreach.

Anti-Phishing Service is open to all CAs – join us!

Flag List (Pt 2) and Collision Update (Pt 3)

What is the Flag List? (London Prot. Part 2)

Provides a list of Organizations or common names…

- Proactive advisory for additional scrutiny – *Not a blacklist*
- Can be used for all CA's to have a shared source to search for High Risk Certificate Requests
- flags for further investigation before issuing
- are automatically updated from trusted sources
    - OFAC is ready to go
- CAs will be able to edit entries when they identify an issue, with reason.
- entries expire with time depending on source

Flag List Policy

Seriousness Level 1-3

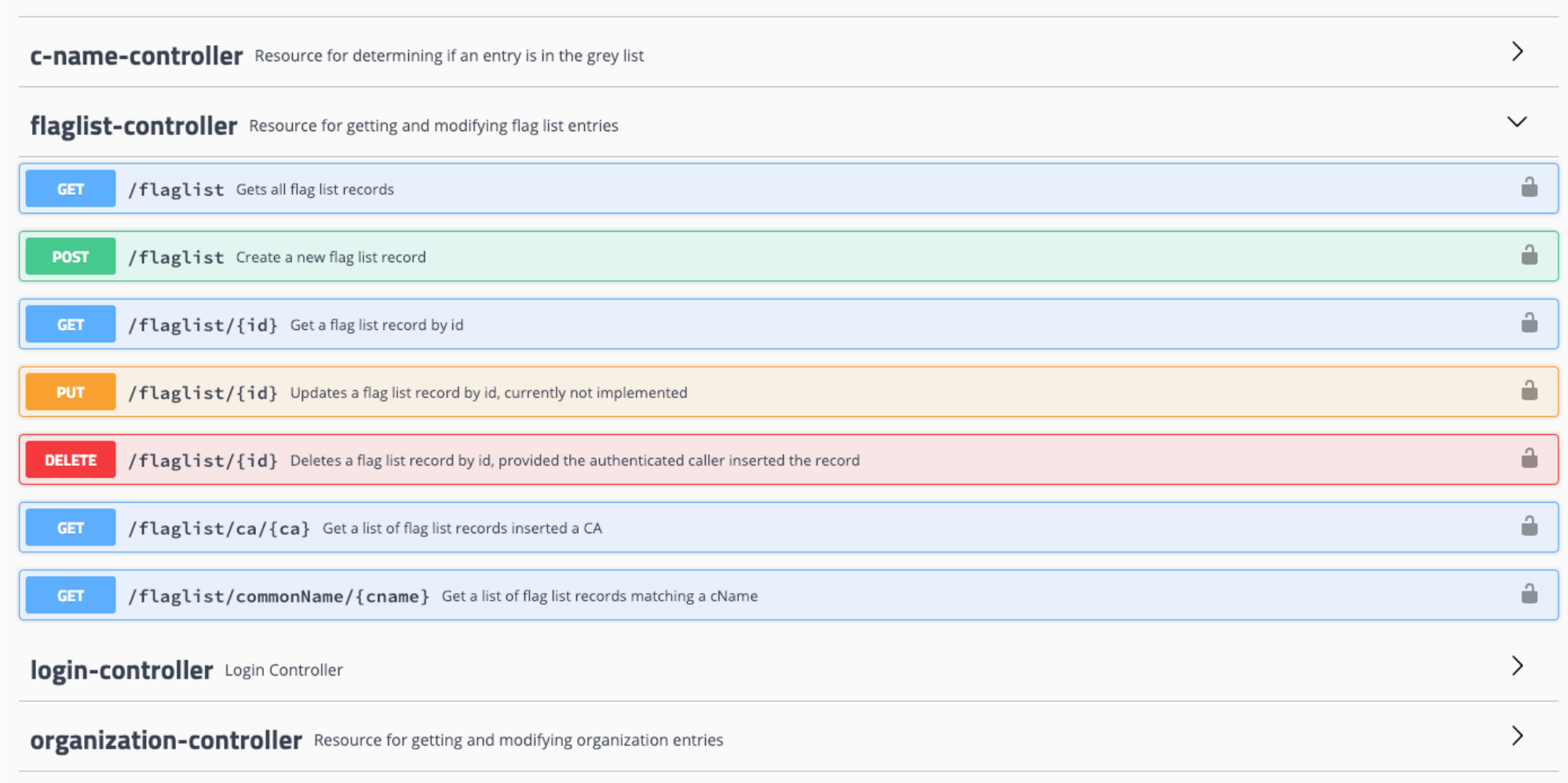
Rev 1 List Members

- Level 3 – High Attention
  - OFAC List (updated daily)
- Level 2 – Medium Attention
  - Phishbank (updated daily)
- Level 1 – Low Attention
  - Certificate Authority reported issue.
  - Alexa top 100 (updated monthly)

Certificate Authority Procedure

- If “flagged”
  - Increase scrutiny on the Company/Domain
  - Review seriousness and list origin
  - CA-decided if they should proceed

Flag List API Implementation



Collision Notification API (London Prot. Part 3)

- Data store of certificates that have already been issued
- Searchable by organization or common name
    - Optional country or country and region/state
- Strict matching
    - We are building regional matching and format checking.
- Work in progress. Looking for partners to collaborate in build process.

Transparency (London Prot. Part 4 - NEW)

- Transparency (as to data sources used for EV validation of SubjectDN data) – *in development.* Will include:
  - Data store of certificates that have already been issued
  - Searchable by organization or common name
    - Optional country or country and region/state
  - Strict matching
    - We are building regional matching and format checking.
  - Work in progress. Looking for partners to collaborate in building process.

FINE PRINT / WHO'S IN

Antitrust Laws; Withdrawal by CAs: The participating CAs will comply with all applicable antitrust laws, including the limitations specified by the Antitrust Notification read aloud prior to CA/Browser Forum meetings.

Participating CAs may withdraw from this Protocol at any time upon notice to the other participating CAs.

- Buy Pass
- D-Trust
- Entrust Datacard
- GlobalSign
- GoDaddy
- Sectigo
- Trustwave

This voluntary Protocol is open to all CAs ***Join us!***

Thank you!

Questions?

Entrust Datacard™