Entrust Datacard
Trusted Identities | Secure Transactions

Entrust Datacard
Corporate Headquarters
1187 Park Place
Shakopee, MN 55379
USA

May 4, 2018

RE: Comments on the Interim Plan

Dear ICANN Board of Directors:

I am writing to you on behalf of Entrust Datacard, www.entrustdatacard.com, a Certification Authority (CA) which is a Member of the CA/Browser Forum (CABF) www.cabforum.org, and also a member of the CA Security Council (CASC), www.casecurity.org.

We understand that ICANN is considering allowing registrars and registries to block access to complete WhoIs / RDAP domain registration data, such as the name and location of the Registrant as well as email addresses and phone numbers for important Registrant contacts such as Registrant, Admin, and Tech (collectively referred to in this letter as "Domain Registration Data"). We also understand that ICANN is considering allowing continuing access to Domain Registration Data for certain critical groups, such as law enforcement and researchers.

OUR REQUEST TO ICANN

We are writing to you with this strong request: **Please do not allow registrars and registries to shut off CA access to full Domain Registration Data**. Please continue to allow CAs the same access to Domain Registration Data as you do for law enforcement and researchers.

As a related matter, there are certain CA service companies that aggregate the WhoIs data from multiple registrars and registries to make it easier for CAs to access the data that comes from multiple sources (services such as Domain Dossier, etc.). We also ask you to continue to allow these CA service companies to access the full Domain Registration Data for use by CAs, subject to any appropriate limitations on use of the data you may impose.

HOW CAs USE DOMAIN REGISTRATION DATA

As you may know, CAs must first validate domain ownership or control before issuing a SSL/TLS digital certificate that website owners use both to encrypt communications with the website and to identify that the website's actual address is the validated domain – *this is a critical part of internet security today*.

The rules for how CA's must complete domain validation are listed at Section 3.2.2.4 of the CA/Browser Forum's Baseline Requirements (BRs), which I have helped write over the past decade. See the full text of BR 3.2.2.4 attached to this letter. There are currently 11 alternative domain validation methods allowed, and 3 of these 11 alternatives require CA access to the WhoIs record for the customer's domain – Methods 1, 2, 3:

BR 3.2.2.4.1 - Validating the Applicant as a Domain Contact

BR 3.2.2.4.2 - Email, Fax, SMS, or Postal Mail to Domain Contact

BR 3.2.2.4.3 - Phone Contact with Domain Contact

See Appendix A for details of these domain validation methods which use WhoIs data.

These WhoIs methods are preferred because they are quick and easy for most website owners – they only need to be listed in WhoIs as the owner of the website, or click approval in an email from the CA for a certificate request, or give approval over the phone. These are the original methods for proving domain ownership or control, and have been used successfully by website owners and CAs for more than 20 years. In addition, these WhoIs methods are generally the favored method by many large enterprise customers, who may have thousands of servers and hundreds of domains in dozens of countries and which must be revalidated periodically.

It's true there are other domain validation methods that don't rely on WhoIs data – for example, requiring the domain owner to put a Random Value received from a CA in a specific location of a web page or a DNS record, which is then confirmed by the CA before issuing the certificate for the domain. However, these other methods don't work well for many website owners:

- Some domain owners are not technologically savvy, and have some difficulty performing the validation steps correctly.

- These alternate methods won't work if the website is not up yet, which may be because the domain owner is launching a new product or name and wants to get a certificate before the website becomes public.

- Some website owners need certificates for non-public sites they maintain behind their corporate firewall – and CAs have no way of looking at those websites to confirm they have posted the required Random Value on the specific page that was designated.

- Large enterprises may find it difficult to post a Random Value in a specific place on every website or DNS record they maintain around the world – in some cases, they may be dealing with many dozens of hosting facilities around the world, and it's difficult to communicate the process correctly in all these places.

For all these reasons, it's important to make sure complete WhoIs data is available to CAs for the purpose of issuing certificates upon request by website owners – WhoIs data is a fundamental part of internet security for encryption.

Arguments for Making WhoIs Data Unavailable to the Public; Exceptions

We recognize there are valid reasons for making WhoIs data unavailable to the public, including privacy reasons (which is not as important to corporations as opposed to natural persons) and also to combat spam. For this reason, it may be appropriate to hide WhoIs data in most cases.

However, CAs who issue SSL/TLS certificates to the owners of the websites should continue to have access to the WhoIs data because they use it to provide a valuable security service to the domain owners, and only at the request of the domain owners.

This is not a case of using WhoIs data for telemarketing, spamming, etc., but instead for providing requested security services and validating an owner's domains using a specific domain validation method selected by the domain owner itself that utilizes the WhoIs data. For this reason, CAs should be added to the list of others (law enforcement, researchers, etc.) who will have continued access to WhoIs data.

Impact of GDPR

We understand that ICANN's proposed rules on hiding WhoIs data are influenced in part by the requirements of the GDPR – and that is appropriate. However, here are factors to consider in the case of ongoing CA access to WhoIs data:

- SSL/TLS digital certificates are almost always ordered by businesses, not natural persons. Likewise, nearly all domains we have researched in WhoIs are owned by businesses, not natural persons.

- The GDPR only applies to natural persons within the EU's stated jurisdiction – the great majority of domain / website owners who order certificates from us and other CAs are not located in the EU, and so should not be subject to GDPR requirements.

- Our company, and every other CA we are aware of, is already making preparations in our own systems and operations to follow the GDPR rules where they apply. This means that after May 25 we will be applying our own algorithms against our own data to make certain we are correctly following GDPR rules for our customers where the rules apply. For this reason, it's not necessary to cut off CA access to WhoIs data to enforce the GDPR – if we encounter data of a natural person covered by the EU regulations when we access WhoIs data to issue certificates, we will stop the process and follow the GDPR rules ourselves. We believe all other CAs are making similar preparations for strong GDPR compliance.

For all these reasons, ICANN should require registrars and registries to provide continued access to WhoIs data for Certification Authorities. In many ways CAs are like "researchers" who will also have continued WhoIs data access (we assume this includes anti-phishing organizations such as the Anti-Phishing Working Group (APWG), PhishLabs, Google Safe Browsing, and Microsoft Smart Screen, who must have WhoIs domain registration data available in order for their anti-phishing algorithms to work and phishing sites to be flagged for user security). Some registries already give CAs WhoIs data access through a "whitelist" process based on the CA's IP address, and this is working well.

For this reason alone, CAs should be given continued access to WhoIs data in the "researcher" category.

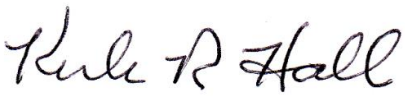
Conclusion

Please give our request for continued CA access to WhoIs data careful consideration. If you agree with this request, please let me know and I will forward your decision to other Certification Authorities around the world through the CA/Browser Forum. (I am current

Chair of the Forum, but am sending you this letter on behalf of Entrust Datacard alone, and not on behalf of the Forum.)

I will be happy to provide additional information on request. Thanks, and best regards.

Very truly yours,



Kirk R. Hall
Director Policy and Compliance – SSL

REDACTED
REDACTED

c: CA/Browser Forum
CA Security Council

Appendix A – Excerpt from CA/Browser Forum Baseline Requirements v1.5.7

https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.5.7-29-Apr-2018.pdf

BR 3.2.2.4 Validation of Domain Authorization or Control

This section defines the permitted processes and procedures for validating the Applicant's ownership or control of the domain.

The CA SHALL confirm that prior to issuance, the CA has validated each Fully-Qualified Domain Name (FQDN) listed in the Certificate using at least one of the methods listed below.

Completed validations of Applicant authority may be valid for the issuance of multiple Certificates over time. In all cases, the validation must have been initiated within the time period specified in the relevant requirement (such as Section 4.2.1 of this document) prior to Certificate issuance. For purposes of domain validation, the term Applicant includes the Applicant's Parent Company, Subsidiary Company, or Affiliate.

CAs SHALL maintain a record of which domain validation method, including relevant BR version number, they used to validate every domain.

Note: FQDNs may be listed in Subscriber Certificates using dNSNames in the subjectAltName extension or in Subordinate CA Certificates via dNSNames in permittedSubtrees within the Name Constraints extension.

3.2.2.4.1 Validating the Applicant as a Domain Contact

Confirming the Applicant's control over the FQDN by validating the Applicant is the Domain Contact directly with the Domain Name Registrar. This method may only be used if:

1. The CA authenticates the Applicant's identity under BR Section 3.2.2.1 and the authority of the Applicant Representative under BR Section 3.2.5, OR

2. The CA authenticates the Applicant's identity under EV Guidelines Section 11.2 and the agency of the Certificate Approver under EV Guidelines Section 11.8; OR

3. The CA is also the Domain Name Registrar, or an Affiliate of the Registrar, of the Base Domain Name.

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names. For certificates issued on or after August 1, 2018, this method SHALL NOT be used for validation, and completed validations using this method SHALL NOT be used for the issuance of certificates.

3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact

Confirming the Applicant's control over the FQDN by sending a Random Value via email, fax, SMS, or postal mail and then receiving a confirming response utilizing the Random Value. The Random Value MUST be sent to an email address, fax/SMS number, or postal mail address identified as a Domain Contact.

Each email, fax, SMS, or postal mail MAY confirm control of multiple Authorization Domain Names.

The CA MAY send the email, fax, SMS, or postal mail identified under this section to more than one recipient provided that every recipient is identified by the Domain Name Registrar as representing the Domain Name Registrant for every FQDN being verified using the email, fax, SMS, or postal mail.

The Random Value SHALL be unique in each email, fax, SMS, or postal mail.

The CA MAY resend the email, fax, SMS, or postal mail in its entirety, including re-use of the Random Value, provided that the communication's entire contents and recipient(s) remain unchanged.

The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation. The CPS MAY specify a shorter validity period for Random Values, in which case the CA MUST follow its CPS.

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.3 Phone Contact with Domain Contact

Confirming the Applicant's control over the FQDN by calling the Domain Name Registrant's phone number and obtaining a response confirming the Applicant's request for validation of the FQDN. The CA MUST place the call to a phone number identified by the Domain Name Registrar as the Domain Contact.

Each phone call SHALL be made to a single number and MAY confirm control of multiple FQDNs, provided that the phone number is identified by the Domain Registrar as a valid contact method for every Base Domain Name being verified using the phone call.

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.4 Constructed Email to Domain Contact

Confirm the Applicant's control over the FQDN by (i) sending an email to one or more addresses created by using 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' as the local part, followed by the at-sign ("@"), followed by an Authorization Domain Name, (ii) including a Random Value in the email, and (iii) receiving a confirming response utilizing the Random Value.

Each email MAY confirm control of multiple FQDNs, provided the Authorization Domain Name used in the email is an Authorization Domain Name for each FQDN being confirmed

The Random Value SHALL be unique in each email.

The email MAY be re-sent in its entirety, including the re-use of the Random Value, provided that its entire contents and recipient SHALL remain unchanged.

The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation. The CPS MAY specify a shorter validity period for Random Values.

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.5 Domain Authorization Document

Confirming the Applicant's control over the FQDN by relying upon the attestation to the authority of the Applicant to request a Certificate contained in a Domain Authorization Document. The Domain Authorization Document MUST substantiate that the communication came from the Domain Contact. The CA MUST verify that the Domain Authorization Document was either (i) dated on or after the date of the domain validation request or (ii) that the WHOIS data has not materially changed since a previously provided Domain Authorization Document for the Domain Name Space. For certificates issued on or after August 1, 2018, this method SHALL NOT be used for validation, and completed validations using this method SHALL NOT be used for the issuance of certificates.

3.2.2.4.6 Agreed-Upon Change to Website

Confirming the Applicant's control over the FQDN by confirming one of the following under the "/.well-known/pki-validation" directory, or another path registered with IANA for the purpose of Domain Validation, on the Authorization Domain Name that is accessible by the CA via HTTP/HTTPS over an Authorized Port:

1. The presence of Required Website Content contained in the content of a file. The entire Required Website Content MUST NOT appear in the request used to retrieve the file or web page, or
2. The presence of the Request Token or Random Value contained in the content of a file where the Request Token or Random Value MUST NOT appear in the request.

If a Random Value is used, the CA SHALL provide a Random Value unique to the certificate request and SHALL not use the Random Value after the longer of (i) 30 days or (ii) if the Applicant submitted the Certificate request, the timeframe permitted for reuse of validated information relevant to the Certificate (such as in Section 4.2.1 of these Guidelines or Section 11.14.3 of the EV Guidelines).

Note: Examples of Request Tokens include, but are not limited to: (i) a hash of the public key; (ii) a hash of the Subject Public Key Info [X.509]; and (iii) a hash of a PKCS#10 CSR. A Request Token may also be concatenated with a timestamp or other data. If a CA wanted to always use a hash of a PKCS#10 CSR as a Request Token and did not want to incorporate a timestamp and did want to allow certificate key re-use then the applicant might use the challenge password in the creation of a CSR with OpenSSL to ensure uniqueness even if the subject and key are identical between subsequent requests. This simplistic shell command produces a Request Token which has a timestamp and a hash of a CSR. E.g. echo date -u +%Y%m%d%H%M sha256sum <r2.csr | sed "s/[-]//g" The script outputs: 201602251811c9c863405fe7675a3988b97664ea6baf442019e4e52fa335f406f7c5f26cf14f The CA should define in its CPS (or in a document referenced from the CPS) the format of Request Tokens it accepts.

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.7 DNS Change

Confirming the Applicant's control over the FQDN by confirming the presence of a Random Value or Request Token for either in a DNS CNAME, TXT or CAA record for

either 1) an Authorization Domain Name; or 2) an Authorization Domain Name that is prefixed with a label that begins with an underscore character.

If a Random Value is used, the CA SHALL provide a Random Value unique to the Certificate request and SHALL not use the Random Value after (i) 30 days or (ii) if the Applicant submitted the Certificate request, the timeframe permitted for reuse of validated information relevant to the Certificate (such as in Section 3.3.1 of these Guidelines or Section 11.14.3 of the EV Guidelines).

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.8 IP Address

Confirming the Applicant's control over the FQDN by confirming that the Applicant controls an IP address returned from a DNS lookup for A or AAAA records for the FQDN in accordance with section 3.2.2.5.

Note: Note: Once the FQDN has been validated using this method, the CA MAY NOT also issue Certificates for other FQDNs that end with all the labels of the validated FQDN unless the CA performs a separate validation for that FQDN using an authorized method. This method is NOT suitable for validating Wildcard Domain Names.

3.2.2.4.9 Test Certificate

Confirming the Applicant's control over the FQDN by confirming the presence of a non-expired Test Certificate issued by the CA on the Authorization Domain Name and which is accessible by the CA via TLS over an Authorized Port for the purpose of issuing a Certificate with the same Public Key as in the Test Certificate.

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.10. TLS Using a Random Number

Confirming the Applicant's control over the FQDN by confirming the presence of a Random Value within a Certificate on the Authorization Domain Name which is accessible by the CA via TLS over an Authorized Port.

3.2.2.4.11 Any Other Method

This method has been retired and MUST NOT be used.

3.2.2.4.12 Validating Applicant as a Domain Contact

Confirming the Applicant's control over the FQDN by validating the Applicant is the Domain Contact. This method may only be used if the CA is also the Domain Name Registrar, or an Affiliate of the Registrar, of the Base Domain Name.

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.