

**Christmas Island Domain Administration Limited ( cxDA)**

**HIGH RISK REGISTRATIONS IDENTIFICATION**

**PROACTIVE ABUSE MITIGATION**



Tools provided by: CoCCA 

The text 'Tools provided by: CoCCA' is followed by the CoCCA logo, which consists of five vertical bars of varying heights and colors (yellow, orange, red, orange, yellow).

ICANN56 | HELSINKI

## *Initial Try 2012*

### **Mandatory manual domain activation with the central registry**

#### **Enforcement**

- Registrants received an email from the registry with a one-use link
- The link lead the registrant ( or admin ) back to the registry where they had to confirm their contact information and agree to the TLD policy
- Until they did so the domain remained un-delegated

#### **Goals**

Ensure the registrant email was valid/active

Ensure the registrant agreed with the AUP and other TLD policy

#### **Problems**

- The Registrant, having registered the domain via a registrar or reseller often did not recognize the sender ( the registry ) and was confused or suspicious
- The email was lost in spam folder and never received, forcing the registrar to activate a domain on behalf of the Registrant
- Reputation or risk factors were ignored

## *Refinement 2014*

### **Escrow deposits inspection against abuse databases (paid service)**

#### **Implementation**

Daily escrow deposits (already being made in ICANN gTLD format) were inspected and compared against various abuse databases by the escrow agent ( NCC)

The email notification was sent to the registrant in case of any possible abuse.

#### **Drawbacks**

- No integration into the registry system ( requires abuse staff to read and interpret the daily emails ), abuse data is not stored in the registry.
- Significant delays between the registration, deposit and the abuse notification.
- It did not prevent abuse, it simply prevents abuse from occurring for an extended period.

## *Refinement 2016*

### **Automatic activation for low-risk registrations.**

#### **Implementation**

Domain registration flow is unchanged from the perspective of the registrar, but domains are not delegated until checked against the Secure Domain Foundation database.

Using the SDF API, the registry operator can identify high-risk from low-risk registrations shortly after registration ( within a minute ). Low-risk domains are automatically delegated, *high-risk domain are flagged for manual activation.*

#### **Benefits**

No delay in delegation for domains that are considered low-risk.

Significant reduction in the registry – registrant communications - which can cause confusion on the part of the registrant and increases the manual workload for registrars.

An additional step allows registry review the high risk transactions manually if desired.

## *What CoCCA looks for at registration and renewal*

### **E-mail**

Has the **full email address** ( name@domain .tld ) been associated with abuse ?

CoCCA will then dig a little further ...

- Has the **domain or user name** associated with any of the contacts the email been associated with abuse ?
- Has the **mx server** associated with domain been associated with abuse ?

### **Name Servers**

Has the name server, or the name server IP address been associated with abuse ?

## *What CoCCA looks for in manual activations*

- CoCCA tracks / logs the IP address of the entity activating the domain.
- IP is checked against the SDF database
- When IP is associated with abuse an administrator at the registry level ( or the registrar depending on the policy matrix) will be required to activate the domain.

## *Continuous Scans*

In addition to the checks shortly after registration or renewal, CoCCA performs a continuous scan of the SDF database and comparison with the SDF database so that if there is evidence of abuse after registration it will be picked up.

In case any matches, CoCCA sends an email to administrators and abuse agents to review.

## *Policy Considerations*

TLD / registry manager will likely have to assume a more active “trust but verify” role mitigating abuse at the registry level.

This “trust but verify” approach may require some modifications to the registrant agreement (if the TLD manager has one) and / or the registrar agreement.

With the increasing use gateways the registrants often do not know who the registrar is, they are only familiar with the reseller they registered through.

When the registry is communicating with the registrant, if the registrant has registered via a reseller the communication should mention the reseller.

The above is only possible if the registry system allows the registry to create and associate registrations with a reseller as well as the registrar.

# *How to Configure*

The SDF API can be connected to by any registry operator.

If you are using the CoCCA software the SDF integration and activation tools are built-in to the current version available from <https://wiki.cocca.org.nz>

Configuration in CoCCA:

Step 1- Configure the SDF connection

Step 2- Enable "Require Activation" for the zone

Step 3-.Select "High Risk Only" on the Activation configuration page.



## Step 1

### Configuration > External Verification Systems

External Verification Systems No Registrar Selected

Home WHOIS Domains Name Servers Contacts Logins

Username / API Key	External Verification System	Description	IP/Host
dbce5e-b32bXXXXXXXX	SECURE_DOMAINS	SecureDomain	dev.securedomain.org

Edit Record (SecureDomain) Cancel

Verification Type: SECURE\_DOMAINS

API Key: dbce5e-b32bXXXXXXXX

Description: SecureDomain

Host: dev.securedomain.org

Save

## Step 2

### Zone > Details

Tech Contact  Loc Address (Unique)

Registration Status

Require Activation

- Active
- Require Activation
- Suspended
- Excluded
- Block Sunrise
- Rolling Sunrise
- Landrush
- TMCH Sunrise
- TMCH Claims

changes the status

ns will be active after

ion - Domains will be

of registration, and a

domains will be susp

domains will be exclude

Applications for a

approved

- Rolling Sunrise - Domains will be re
- may be made by the registrar or by
- be deleted.

### Step 3

#### Zone > Activation Settings

Home WHOIS Domains Name Servers Con

**Base URL** The base URL for the activation site. This will be put in the email to registrants be used.

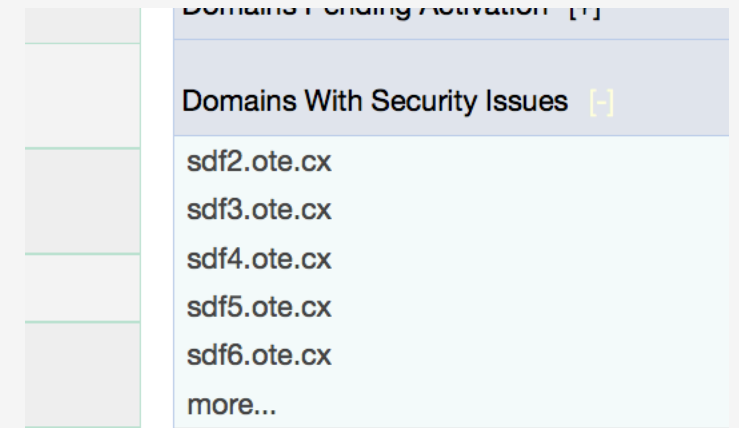
**Completion URL** The URL to send visitors to when they have finished activating their domain. I thank you page. Nothing flash but it says thanks.

**Pending Activation Zone Generation** What should zone generation do with domains pending activation?

**Activate All Domains** *Require Activation for all domains, or just those deemed high risk by the exte*  
 All Domains  High Risk Domains

**Resend Schedule** The activation emails will automatically be resent every so often, until the de- emails being resent.

If a registration is flagged admins will get an email and it will appear in the top Right menu when you login.



# CoCCA Manual Activation Step 1

CoCCA | TLD Registry

## Registrant Agreement and Contact Verification

Dear Garth Miller or Garth Miller,

The continued use of the sdfote10.ote.cx domain requires that all Registrants (or their Administrative contacts) comply at all times with applicable .ote.cx policy. This policy requires that the central registry maintain accurate and reliable information regarding registrants, and also that Registrants agree to be bound by the .ote.cx registrant agreement.

### Part 1 | Verify Registrant Information

The .ote.cx registry has been provided with the following information on 2016-06-25 from Rifaee Konsult:

#### Registrant Details

<b>Name</b>	Garth Miller
<b>E-mail</b>	garth.miller@cocca.org.nz
<b>Phone</b>	0046223232332

#### International Address

<b>Name</b>	Garth Miller
<b>Organisation</b>	COCCA TEST
<b>Address</b>	Garth Miller
<b>City</b>	Garth Miller
<b>Country</b>	DZ

#### Admin Contact Details

<b>Name</b>	Garth Miller
<b>E-mail</b>	garth.miller@cocca.org.nz
<b>Phone</b>	0046223232332

#### International Address

<b>Name</b>	Garth Miller
<b>Organisation</b>	COCCA TEST
<b>Address</b>	Garth Miller
<b>City</b>	Garth Miller
<b>Country</b>	DZ

The information above is:

- Correct  
 Incorrect

[Continue](#)

# CoCCA Manual Activation Step 2

CoCCA | TLD Registry



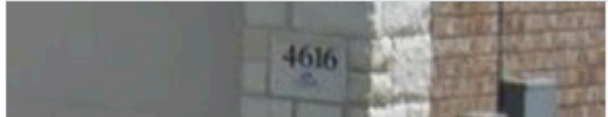
Registrant Agreement and Contact Verification

**Part 2**

**Accept the .ote.cx Registrant Agreement [\[+\]](#)**

**.ote.cx Acceptable Use Policy [\[+\]](#)**

I,  , confirm that as of 2016-06-25 00:18 (UTC), from 69.86.251.193 that I agreed  to be bound by the .ote.cx Registrant agreement above. Your IP will be stored and confirmation of Agreement time and date will become part of the domains permanent history.



[Privacy & Terms](#)