Council of European National Top-Level Domain Registries

White paper

Models of registry lock for top-level domain registries

What is registry lock

Registry lock is a security measure to help registrants protect their domain names from unintended or unauthorised operations at the registry level by adding an advanced / dedicated form of authentication. While this additional authentication can be done at the registry level, some registry lock solutions rely more heavily on the registrar to increase the adoption and ease of use for the registrant. These solutions may therefore not necessarily be referred to strictly as a 'registry lock' but rather a 'registry-assisted' registrar lock.

Objective

A CENTR survey in 2019 found that of the 27 participating ccTLD registries, 14 offer a registry lock feature and 8 are planning to. The primary goal of this document is to help domain name registries (re)design their registry lock service, and thereby achieve greater harmonization in the different registry lock offerings.

Although online security is top of mind for many, CENTR data shows that the number of domains which are protected with a registry lock are generally very low. A possible reason for the low adoption may be due to the fragmented nature of current registry lock services offered by registries. To effectively promote and communicate the value of registry lock, it is important that domain registrars and resellers have a clear, and where possible, uniform approach. Without uniformity the contrasting and highly nuanced offerings from registries may be counterproductive and may decrease the likelihood of adoption.

A group of CENTR member registries have analysed current and planned registry lock services and grouped them into two different models, each with two variants. These models are designed to help registries align their registry lock offerings, thereby reducing the current fragmentation. The technical implementations of these models can be standardized to ease integration with registrars and resellers. This taxonomy will hopefully encourage gradual movement to a more streamlined approach, making the interaction between registry and registrar more predictable.

We describe the business rules and policies of the different models, including the levels of additional security they provide. This can assist registries in deciding which model is appropriate for them, but also align marketing efforts aimed at registrants, again reducing confusion by reducing fragmentation.

Definitions

These definitions are based on the registry perspective of registry lock related operations:

- **initial lock:** the operation of first enabling registry lock on a given domain name (including the appointment of additional trusted contacts for further registry lock operations);

CENTR vzw/asbl
Belliardstraat 20 (6th floor)
1040 Brussels, Belgium

Phone: +32 2 627 5550
Fax: +32 2 627 5559
secretariat@centr.org

www.centr.org

- **unlock or lock termination:** the process of completely and permanently removing registry lock on a given domain name;
- **lock waive:** the action of temporarily removing registry lock protection on a domain name, e.g. to legitimately modify one or several of the domain name properties and/or associated objects;
- **lock restore:** the operation of enforcing all registry lock protection again after the lock waive duration.

Actors involved in the aforementioned operations:

- **selling entity:** the party in charge of promoting and selling the registry lock service to the domain name registrant;
- **initiator:** the actor at the origin of the registry lock operation, this could be either the registrant or one of the appointed trusted contacts;
- **endpoint:** the entity that interacts directly with the registry, either initiating or relaying the registry lock operation request.

Interactions with the registry are classified as either:

- **in-band:** i.e. automated online communications with the registrar, including EPP or any other similar API interface;
- **out-of-band:** all other communication channels, often requiring human interaction, being either online (e.g. e-mail, web panel) or offline (e.g. phone, physical mail).

Based on these definitions, the main separation (between models 1 and models 2) is based on the entity performing the authentication of the initiator of a request:

- models 1A and 1B are deemed to be **registry-focused models** as the registry authenticates the initiator of the registry lock request;
- models 2A and 2B are named **registrar-focused models** as the authentication of the initiator of the request is delegated to the registrar.

The following table depicts the taxonomy we propose for registry lock models.

Category	Item	Model 1A: Registry focused (direct sale)	Model 1B: Registry focused (registrar sale)	Model 2A: Registrar focused (fully delegated)	Model 2B: Registrar focused (manual auth.)
Selling entity		Registry	Registrar	Registrar	
Request endpoint entity	***Initial lock***	Registrant	Registrar	Registrar	
	Unlock	Registrant		Registrar	
	Lock waive	Registrant		Registrar	
	Lock restore	Registrant		Registrar	
Initiator authentication entity		Registry		Registrar	
	Initial lock	Out-of-band	In-band	In-band	In-band/out-of-band

CENTR vzw/asbl · Belliardstraat 20 (6th floor) · 1040 Brussels, Belgium
Phone: +32 2 627 5550 · Fax: +32 2 627 5559 · secretariat@centr.org · www.centr.org

Endpoint authentication method	***Unlock***	Out-of-band	In-band	Out-of-band
	Lock waive	Out-of-band	In-band	Out-of-band
	Lock restore	Out-of-band	In-band	Out-of-band
Endpoint authenticated entity	***Initial lock***	Single (registrant)	N/A	Registrar
	Unlock	Single or several (trusted contacts)	N/A	Registrar
	Lock waive	Single or several (trusted contacts) [*]	N/A	Registrar
	Lock restore	Single or several (trusted contacts) [*]	N/A	Registrar
Processes	***Restore action***	**Implicit**: automatic lock restore after time-based expiration of the registry lock waive		
		Explicit: specific authentication is required to restore registry lock		
	Partial waive	**No:** all changes are possible during the registry lock waive period		
	Request authentication	**Business hours only:** requires scheduling of registry lock waive		
		24/7: registry lock waive scheduling is optional		
	Deletion prevention	**Yes:** Registry lock activation prevents domain deletion even in absence of renewal		

[*] domain name registrar could be a de-facto trusted contact

Registry-focused models

In models 1A and 1B, the registry is in charge of authenticating the initiator of registry lock requests and, most of the time, those requests will come directly from the registrant. These two models mainly differ from a sales channel perspective.

While model 1A only relies on direct registry/registrant interaction and does not involve registrars at all, model 1B allows for the sale of registry lock service via registrars. As a consequence, it also allows registry-lock initiation via in-band communications and therefore requires the extension of this interface to handle registry lock specific requests.

In all cases, authentication for unlocking, lock waive or lock restore is performed by the registry. Authenticated parties are either the registrant (especially for initial lock) or any trusted contact, appointed during the initiation phase.

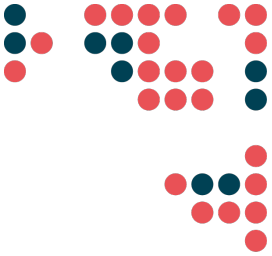
In registry-focused models, interaction with registrars is limited. They will be made aware of the presence and status of registry lock on a given domain via in-band methods like EPP and/or their registrar portal.

Registrar-focused models

In models 2A and 2B the registrars authenticate the initiator of a registry lock request. It is hence left to the registrars to determine by what means this authentication is carried out, possibly framed by a contractual agreement set by the registry. It shall however be noted that registrar-focused models do not protect against a potential security breach at the registrar.

In the first variation (model 2A), the authentication of the initiator is fully delegated to the registrar, and no further authentication is performed by the registry. The registry lock process can hence be fully automated with little or no modification of the existing in-band communication channel (such as EPP). The downside is that registry lock requests

CENTR vzw/asbl · Belliardstraat 20 (6th floor) · 1040 Brussels, Belgium
Phone: +32 2 627 5550 · Fax: +32 2 627 5559 · secretariat@centr.org · www.centr.org



are no more secure than any other automated interaction with the registrar. Many would consider this model to be a form of registrar lock, rather than registry lock, but it is included in this document for completeness.

In the second variation (model 2B), while the registrar authenticates the request initiator and relays the request on its behalf to the registry, further authentication of the registrar is performed at registry level using an out-of-band method (such as a registrar panel or a mail exchange between registry and registrar). This additional step of stronger registrar authentication is added to circumvent breaches due to registrar security being compromised.

Hybrid models

While providing an organised overview of possible registry lock models, the taxonomy presented above does not intent to capture the whole complexity and all business cases related to this service. Hence, while discouraged, hybrid models can exist.

For instance, in registry-focused models, one of the appointed trusted contacts can be the registrar of the domain name, hence blurring the lines with registrar-focused models.

Another example could be the case where lock initiation is made out-of-band with the registry directly authenticating the registrant (as in model 1A) but subsequent requests (for unlock or restore) would go through the registry via in-band communication without further authentication (like in model 2A).

Finally, a registry can decide to deliberately allow both the registrant (e.g. via a registrant web portal) and the registrar (e.g. via an in-band communication method like EPP or via the registrar web panel) to initiate a registry lock request making the registry lock implementation classify as both registry and registrar focused.

Authentication methods - recommendations

This section details recommendations for the authentication of entities as well as the management of appointed trusted users in the context of the registry lock service.

Waive process

A lock can be waived either on a per-transaction basis or on a time-basis.

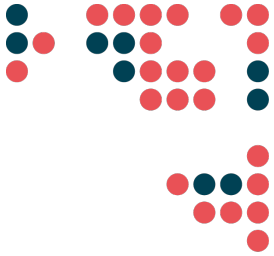
In a per-transaction process, the registrant has to request a certain transaction to be done on a domain name first, after which the authentication process will start. This can be considered the most secure model, as any successful authentication is only valid for a specific approved transaction. However, this may also complicate change management for the registrant, e.g. implementing a roll-back plan, which would need its own, separate authentication process, possibly outside normal business hours. If the authentication process involves a manual action by the registry, this may lead to a requirement for 24/7 access to customer service at the registry.

In a time-based waive process, the registrant first waives the lock, after which any transaction is processed without further authentication, until the lock is reinstated, either manually by the registrant or after a predetermined time period. It is also possible to offer a solution where the registrant can schedule a certain time slot ahead of time where the lock is waived, e.g. for maintenance outside normal business hours.

In-band authentication

In-band communications provides an automated interaction channel between the registry and the registrars. In the case of registry lock requests, we envisage that such exchanges could rely on an extension of the Extended

CENTR vzw/asbl · Belliardstraat 20 (6th floor) · 1040 Brussels, Belgium
Phone: +32 2 627 5550 · Fax: +32 2 627 5559 · secretariat@centr.org · www.centr.org



Provisioning Protocol (EPP) or any similar API. Therefore, the following recommendation is derived to what is applicable or recommended for generic EPP communication:

- use separate credentials (login/password or token) for each authenticated entity;
- restrict access based on source IP address;
- couple credentials and source IP address so a given credential could only be used from a specific source IP address;
- use a secure communication channel (EPP over TLS or HTTPS);
- use client-side certificates in addition to credentials;
- couple client-side certificates with credentials and/or source IP address so a given client-side certificate could only be used with specific credentials and/or a specific source IP address.

Out-of-band authentication

Out-of-band communications rely on separate interaction channels (shared with other services or created specifically for registry lock) that will generally require manual human intervention. We will provide recommendations for both online (web-based, e-mail, …) and offline (mail, phone) methods.

Online methods

For web-based methods (registrant or registrar panel), we recommend a set of security measures similar to in-band authentication methods. Unfortunately, especially when interacting directly with registrants, solutions like source IP restriction or client-side certificates may not be applicable on a large scale. However, as those communication methods allow for manual human intervention, some additional security measures, like two-factor authentication, are recommended:

- use separate credentials (login/password or token) for each authenticated entity;
- use multi-factor authentication with an additional one-time password (OTP) delivered via a physical or software token, TOTP or any other applicable solution;
- if scaling permits, restrict access based on source IP address;
- if scaling permits, couple credentials and source IP address so a given credential could only be used from a specific source IP address;
- use a secure communication channel (HTTPS) extended with modern security measures like HSTS and/or TLSA;
- if scaling permits, use client-side certificates in addition to credentials;
- if scaling permits, couple client-side certificates with credentials and/or source IP address so a given client-side certificate could only be used with specific credentials and/or a specific source IP address.

For email-based exchanges, equivalent levels of security and privacy are recommended. It should be a requirement that both the sender and receiver email domains be secured with SPF, DKIM and/or DMARC. Messages should be signed (for requests) and encrypted (for password delivery) using for instance PGP. The required key exchange should therefore have been operated using an offline method.

CENTR vzw/asbl · Belliardstraat 20 (6th floor) · 1040 Brussels, Belgium
Phone: +32 2 627 5550 · Fax: +32 2 627 5559 · secretariat@centr.org · www.centr.org

Offline methods

Offline methods have the advantage of being safe from security breaches due to improper technical implementation of security protocols, but they are still open targets for social engineering. It is therefore wise to respect some guidelines and favour the following channels (in decreasing order of trustworthiness):

- in-person interaction with the registrant after proper identification based on official documents (passport, national ID card);
- phone call in addition to other identification credentials shared by a different offline method or an online method;
- fax in addition to other identification credentials shared by a different offline method or an online method.

Mixed methods

Online and offline methods could be mixed for increased security. One can imagine a scenario where the authentication of an appointed trusted contact requires:

- a phone call from the authentication entity to the trusted contact where the contact will have to provide several authentication elements;
- a shared password (or the code from a TOTP physical token) received by registered mail upon appointment;
- a one-time password sent to his/her e-mail during the phone call.

Trusted contacts management

The appointment and management of trusted contacts should be performed while taking care not to weaken the security of the authentication or to put the domain into a dead-lock situation where no party is able to waive or unlock it.

It is therefore encouraged for the related parties to specify clear procedures for the following operations related to trusted contacts management:

- trusted contact appointment, especially during the initiation phase when new contacts are bootstrapped from a single authenticated party;
- trusted contact information update, particularly when the contact needing to be updated is no longer able to authenticate himself due to expired credentials;
- additional trusted contact appointment, considering a maximum number of trusted contacts;
- trusted contact revocation, considering a minimum number of trusted contacts;
- trusted contacts recovery, when no or an insufficient number of trusted contacts is able to authenticate to perform trusted contacts management operations.

CENTR vzw/asbl · Belliardstraat 20 (6th floor) · 1040 Brussels, Belgium
Phone: +32 2 627 5550 · Fax: +32 2 627 5559 · secretariat@centr.org · www.centr.org

This document has been created by a group of CENTR members (see below) and was finalised in August 2020. CENTR thanks all participants to the project for their work and dedication.

Erwin Lansing (DK Hostmaster)

Marc Groeneweg (SIDN)

Piotr Studziński-Raczyński (NASK)

Guillaume-Jean Herbiet (RESTENA DNS-LU)

Sascha Kämpf (DENIC)

Facilitation: Patrick Myles (CENTR)

CENTR vzw/asbl · Belliardstraat 20 (6th floor) · 1040 Brussels, Belgium
Phone: +32 2 627 5550 · Fax: +32 2 627 5559 · secretariat@centr.org · www.centr.org