

Lock States

PAB SUB-COMMITTEE REPORT

1. Introduction

The subject of lock states was first discussed at PAB meeting 58 (July 2008). It was agreed at this meeting that a PAB sub-committee should be formed to discuss this issue and report back to the PAB. A PAB sub committee Chaired by Jarrod Robinson was held on 20 August 2008 and a paper was presented at PAB meeting 59 (September 2008) http://www.nominet.org.uk/digitalAssets/33206_PABSept08_Lock_state_sub_committee_report.pdf.

At the September meeting there was some discussion about the possibility of providing a “renewal” lock so that a registrant could safeguard against their domain name being lost if their registrar didn’t renew it. It was agreed that there should be a further subcommittee to discuss this issue in more detail with a view to making a further recommendation to the Board.

In the discussion on Phishing at meeting 60 (January 2009) it was suggested that there should be a registrar lock to enable a registrar to lock a domain name that is being used for phishing. It was agreed that this suggestion should be discussed by the lock states subcommittee.

Jarrod Robinson volunteered to Chair the sub-committee meeting which was held at Victoria Park Plaza, 239 Vauxhall Bridge Road, London, SW1V 1EQ on 25 February 2009. The sub-committee meeting was attended by Andrew Bennett, Clive Feather, Mark Healey and Michael Toth from the PAB, with Eleanor Bradley and Laura Hutchison attending from Nominet.

2. Why do we need a lock state?

Registrants, especially brand owners, with a portfolio of valuable domain names would like to have the facility to lock their domain names at the Registry level for protection. There is a feeling that this would offer more security in the event of their registrar being hacked. It would also be helpful if registrars and Nominet could have the facility to lock a domain name to prevent repeat abuse of the opt-out facility. It was also suggested that now Nominet has moved to providing the majority of services online, there is a perception that this isn’t as secure as the previous manual system.

3. Existing PAB Recommendations on lock states

The following recommendations were made by the PAB in September 2008:

- Nominet should have a registry lock to be used in line with the domain name terms and conditions as necessary. A registrar should be notified when this is used on a domain name on their tag.
- There should be the function within Registrants Online to allow a registrant to set a lock to prevent the automatic transfer or cancellation (surrender) of their domain name(s) regardless of whether a registrar is subscribed to the lock-state service.
- A registrar should be able choose to allow their registrants access to an extended lock state service via Registrants Online. This should be done in a manner that enhances the registrar channel, for example via a co-branded system (unique to each tag) that allows a registrant to set various locks on their domain name(s) including the function to lock a domain to a particular tag. This service would include the following features:
 - The default of this service would be for all registrars to be opted in and then they can choose to opt out if they wish.
 - When a domain name is moved from an opted-in tag to an opted-out tag through Registrants Online, then the registrant will get a warning that the new registrar doesn’t allow them to set lock states. If the registrant chooses to complete the tag change then all lock state settings will default to being unlocked.
 - When transferring between two opted-in tags then all details currently locked on a domain name will remain locked.

- A registrar should be able to view the locks that are in place on a domain name on their tag and should be notified of any changes.
- A registrar should have the ability to turn on a registrant lock on behalf of their customer but not to turn it off again.
- The tags subscribed to the lock-state service should be regarded as public data and the information made available to all.

4. Renewal lock

At the subcommittee on Lock states in September 2008 the group recommended that a registrant should have the facility to lock the domain name to renew. However, the PAB could not agree with this suggestion and were concerned that this would mean that a registrar would be forced to pay for a domain name that they hadn't actually renewed themselves. The sub committee agreed with this concern and felt that a registrar shouldn't be forced to renew a domain name in this way. However they sub committee group but did feel that there should be an additional layer of protection for registrants to safeguard against a domain name being lost due to not being renewed by a registrar.

The renewal scenarios are:

- i) domain name renewed in advance of expiry;
- ii) "do not renew" flag set by registrar;
- iii) domain name not renewed by expiry date;

The lock state would simply over-ride the scenario when a "do not renew flag" is set and an email reminder would be sent to the registrant (as if the domain name was in scenario iii above).

5. Phishing lock

At the January PAB meeting it was suggested that there should be a facility to lock a domain name that has been used for phishing to prevent it being moved to another registrar. This lock would remove the name servers and prevent any tag change. The lock could only be set and removed by the registrar and it would be explicitly to be used only when a domain name has been used for phishing.

There was concern that this lock could be used maliciously by registrars to lock a domain name to their tag. However, it was agreed that this could be overcome simply by very clear communication to registrars that the lock was only to be used on domain names associated with phishing and any abuse of the facility would be dealt with severely by Nominet.

Another concern was that a registrar would be liable if they mistakenly locked a domain name that turned out not to be involved in phishing. It was argued that registrars still have the same risk at the moment as they remove name servers from a domain name suspected of phishing. To minimise the risk of disruption for a site incorrectly locked as a phishing site, it was suggested that the lock could only block the domain name for 24 hours. However, the consensus was that phishing emails would have a longer life than this and people could still be trying to access the site after 24 hours.

6. Lock state sub-committee recommendations

The lock state sub-committee agreed to make the following recommendations to the PAB:

Nominet should implement a "Please notify me if my registrar doesn't renew my domain name" lock. This causes the system to act as though the DNR flag is not set and a reminder email will go to the registrant to notify them that the domain name is due for renewal. The lock can only be set and removed by the registrant.

Nominet should implement a Phishing lock to allow a registrar to lock a domain name that has been used for phishing. This would remove the name servers and prevent the domain name being moved to another tag. It will be clearly stated to registrars that this lock is only to be used in cases of phishing and that abuse will be severely punished. This lock will be introduced for a six-month trial period and usage will be carefully monitored during this period.