Direct UK Registrations

Response to Consultation Document

Author: Alex Bligh
Date: 4th January 2013

A. Executive Summary of Response

This document is a response to the consultation document entitled "Consultation on a new .uk domain name service" published by Nominet in October 2012. It should be read in conjunction with my specific responses to the questions asked within the document. Section numbering in the remainder of this document corresponds to the section numbering within Nominet's own document. This section A summarises my consultation response.

This is consultation document is one of the least well thought-out proposals I have yet to read from Nominet. Whilst there are a number of problems with the detail of the proposal, there are two significant and overarching problems: conflation of purpose, and naivety as to the proposed mechanisms.

A.1 Conflation of purpose

The first problem is that it conflates two entirely separate issues:

- The question of whether direct registrations should be capable of being made at the *.uk* level; and

- The question of whether Nominet should encourage more 'secure' registrations (validated contact address details, virus checks, DNSSEC and so on), and if so under what circumstances and under what commercial terms.

Nowhere in the consultation document does Nominet adequately explain why registrants within the existing subdomains should not be able to avail them of the 'high security' registrations, and why it is thus in the interests of Nominet's stakeholders to require such registrants to re-register another domain within *.uk*, at considerable cost to them. As such costs involve not payments to Nominet and/or the registrar concerned, but also the far larger costs of re-branding, it seems perverse not to provide such 'high security' registrations where possible in *.uk*. A cynic might suggest this was simply a revenue or empire building exercise.

Equally, nowhere in the consultation document does Nominet adequately explain why the first-come first-served light-weight registration model which has served Nominet well from inception should not be available within direct registrations in *.uk* (assuming opening up *.uk* for third party registrations is a good idea). Nominet proposes that *.uk* be a domain with enhanced checking of registration details (including the rather quaint idea of sending letters by post). Nominet has already tried this model with (e.g.) *ltd.uk* and *plc.uk*. Whilst I cannot find current information on Nominet's web site, I believe these subdomains are less than 1% of the size of *co.uk* and considerably smaller than (say) *org.uk*.

The only purported link is the one set out at the head of the next section, which is in my opinion laughably naïve.

A.2 Naivety of mechanism

The only arguable link between the two issues set out in A.1 above is that consumers will somehow draw a link between the fact that the web site they visit or email they receive has the domain name '*example.co.uk*' or '*example.plc.uk*' and conclude that is insecure (being registered as third level domains within existing SLDs), but also know that '*example.bt.uk', 'example.pcl.uk'* (*sic*) or '*exampleplc.uk'* are secure (being registered as second level domains within the *.uk* subdomain). This seems fantastically unlikely unless Nominet embarks on a world wide education program of its own domain registration structure.

Nominet appears to be around 15 years out of date in this area. Consumers increasingly do not recognise domain names at all, but rather use search engines. The domain name is becoming increasingly less relevant (despite Nominet's research) as consumers are educated to 'look for the green bar' or 'padlock'. Whilst SSL certification has many weakness in proving security, it is by no means as poor a solution as the solution Nominet proposes to replace it.

A.3 Recommendations

I make the following recommendations:

1. Nominet should abandon its current proposals in their entirety.

2. Nominet should disaggregate the issue of registrations within *.uk* and the issue of how to help build trust in *.uk* in general. Nominet should run a separate consultation for opening up *.uk*, as a simple open domain with the same rules as *co.uk*. There are plenty of arguments for and against this, but the current consultation confuses them with issues around consumer trust. Whilst consumer trust and so forth are important, they are orthogonal to this issue.

3. Nominet should remember that a core constituency of its stakeholders are those who have registered domain names. If new registrations are introduced (permitting registration in *.uk* for instance), Nominet should be sensitive to the fact that these registrants will feel compelled to reregister if only to protect their intellectual property. Putting such pressure and expense on businesses to reregister is one thing (and a matter on which subject ICANN received much criticism in the new gTLD debate); pressurising them to reregister and rebrand by marketing their existing *co.uk* registration as somehow inferior is beyond the pale (for instance marketing as 'less secure' as proposed here). Any revised proposal for opening up *.uk* should avoid this.

4. Nominet should recognise that there is no silver bullet (save perhaps one used for shooting oneself in the foot) for the consumer trust problem, and hence it will have to be approached incrementally.

5. Nominet should be more imaginative and reacquaint itself with developments in technology and the domain market place. Nominet's attempt to associate a particular aspect of consumer trust with a domain name is akin to attempting to reinvent the wheel, but this time with three sides. Rather, Nominet should be looking at how to work with existing technologies. For instance, if Nominet was really interested in providing enhanced security, it could issue wildcard domain validated SSL certificates for every registration to all registrants; given Nominet already has the technology to comprehensively validate who has a domain name, such certificates could be issued cheaply or for free (and automatically). This might make Nominet instantly the largest certificate issuer in the world. If Nominet wanted to further validate users, it could issue EV certificates. And it could work with emerging

technologies such as DANE to free users from the grip of the current overpriced SSL market.

B. Why are we consulting?

B.1 I agree with this section. I commend Nominet on the long consultation period.

C. What do you need to do?

C.1 I have no comments on this section.

D. Next steps

D.1 I commend Nominet on the long consultation period. However, my view is that these proposals if they are not to be abandoned entirely require substantial rewriting. As such they should go out to consultation again, rather than be introduced with 30 days' notice.

E. Background

E.1 Making 'ensur[ing] that our activities support the development of a UK internet space that helps create economic growth and that is as safe, secure, reliable and trusted as possible' is a laudable objective; however, it requires context. First, end users are not the only stakeholders (registrants are stakeholders too). Secondly, Nominet needs to ensure the route to achieve such safety, security, reliability and trust is both fair and economically prudent, particularly for registrants. Consumer protection should not be the be-all and end-all. Nowhere within the background section are the rights or interests of registrants adequately considered. Registrars' interests are not even mentioned.

E.2 This section is full of unevidenced assertions and poor logic. For instance this paragraph is entirely unevidenced:

> *'We believe there is a real opportunity to support the development of the digital economy by creating a specialised .uk domain name service that can support UK business online, and which would in turn enhance consumer trust and confidence through features that ensure greater security and verification of registrant contact details. We also believe that consumers would benefit from the knowledge that the business they are dealing with has verified contact details in the UK. This proposed service would meet the needs of those businesses that wish to have an online presence that demonstrates their commitment to online security and trust. It therefore has the potential to have a substantially positive effect on the digital economy in encouraging business online.'*

Each of those sentences requires evidence if to be taken seriously. They also do not form a logical chain. For instance, no evidence is presented that a specialised *.uk* domain service would enhance consumer trust and confidence. Were it the case that new registration domains enhanced consumer trust and confidence, Nominet would

presumably be able to point to data concerning new gTLD introduction where consumer trust and confidence has been enhanced, or indeed to the introduction of its own SLDs in the past. To my knowledge, there is no such data. The absence of such data means Nominet bears the burden of proof that there is something special about its proposal to set it apart from what appear to be examples to the contrary.

Nominet states that consumers would benefit from the knowledge that the business they are dealing with has verified contact details in the UK. I accept that this is true. However, it is unlikely Nominet's proposal will provide this, as all the consumer will see is something very slightly different in their browser URL bar or email client. How will the average computer user be able to differentiate between an address ending *.uk* which has these verified contact details and an address ending in *.uk* that does not? To achieve this the computer user would first have to know about Nominet's peculiar scheme, and secondly have to know which second-level items are SLDs and which are registrations. How are they to know that '*www.net.uk'*, '*www.me.uk'*, '*www.co.uk'*, and '*www.org.uk*' are qualitatively different from '*www.inet.uk*', '*www.you.uk*', and '*www.charity.uk*'? How are they to know that '*example.co.uk'* has no address validation, '*example.ltd.uk*' has another (must be registered to a UK company), and '*example.company.uk*' has yet another? Or that '*example.co.uk*' and '*example.plc.uk*' are 'insecure' in some sense, but '*example.bt.uk', 'example.pcl.uk'* (*sic*) or '*exampleplc.uk'* are secure? This makes no sense at all.

Moreover, the consumer already has a way of telling whether a site has UK contact details. They click on the padlock in their browser. If they are doing business without SSL, Nominet should be advising them not to.

Further, that a site has UK contact details does not demonstrate that it is bona-fide, or the site that the user thinks they are dealing with. The trust problem is not related to what country the registrant's contact details are in, it is related to verifying that the purported site owner is who (and perhaps where) it says it is, so that the consumer can make an informed decision of whether to deal with him, be they in the UK, France, or Russia. Certificates are the obvious way to do that. If Nominet really thinks domain names are that important without SSL, I suggest it writes or finds and existing set of browser plug-in that retrieves the 'whois' information for the domain, and then ensures that whois data is accurate. None of this requires opening up another domain.

Lastly, Nominet appears to have omitted to consider any of the disadvantages of its proposals, such as the cost (particularly to existing registrants). The failure to present a balanced argument undermines the credibility of the document as a whole.

E.3 Nominet argues at the head of the second column that introduction of new TLDs is likely to cause confusion, but fails to recognise that *any* significant change to *.uk* is likely to cause the same confusion to an extent.

E.4. Nominet argues:

> *'Consumers and businesses have often asked us the reason why we register domains in co.uk and org.uk instead of .uk. The reasons for the structure of the .uk namespace are historical, although many other countries like France and Germany, register domains as example.fr and example.de, whilst others such as Japan offer both example.jp and example.co.jp. A significant and growing number of countries, as well as forthcoming new generic top level domains, are offering a shorter domain suffix, either alone or alongside closed or managed second level domains, indicating a trend for shorter*

domain names. This proposed direct.uk service will allow domain names to be registered directly at the second level such as example.uk.'

This is true, as far as it goes. However, it fails to argue why such direct registrations should be linked to the alternative registration practices suggested. Equally, and more importantly, it fails to address the reason why registration at *.uk* has not been opened up, which is the difficulty with respect to existing registrants in terms of cost of reregistration and rebranding. If it were as simple argument as Nominet suggests, ICANN would simply have opened the root for all to register in.

E.5. Nominet argues:

'Finally, we are fully committed to continuing to support the existing portfolio of second level domains that we manage such as .co.uk and org.uk, as well as those managed by third parties and are not proposing any changes to those spaces.'

This misses the point entirely. Of course existing registrations will be supported. However, businesses will need to protect their IP by registering in *.uk* in addition to their current *co.uk* registrations. Put aside for a minute the hassle involved. Not only does that raise the potential of cybersquatting and disagreements between multiple bona-fide holders of IP relating to the same domain name, but worse still it paints the existing registrants as having somehow 'insecure', 'unsafe' or 'untrustworthy' domains which would put pressure on them to rebrand. All for a supposed security, safety or trustworthiness which will be largely imaginary.

E.6 Nominet seems to be under the impression that safety is to be found dealing with UK organisations. Given the harmonised consumer law (see e.g. distance selling directive) when dealing with other EU states, this seems a rather old fashioned distinction. I'd suggest it might also be an unlawful distinction.

F. About You

F.1 See online response for personal details.

F.2 I hereby permit and encourage Nominet to publish this response unedited in full.

G. Security

G.1 This section takes a very narrow view of security. The single most important security provision that a site can have is an SSL certificate. This ensures that the site the user is accessing has been certified by the certificate issuer as being operated by the body in receipt of the certificate. It also ensures (through the use of the https protocol) that the user's traffic (including passwords and other sensitive data) is not being eavesdropped upon. Unbelievably, nowhere in this section does Nominet even mention SSL. Nor does it mention any other common security problems (such as inadequate storage of personal data by the site owner) or sensible provisions for users to take (such as not using the same password on each site); instead it concentrates on a single provision, malware scanning.

G.2 Instead it recommends its own dubious 'trust mark' provision, which will be incapable of automatic enforcement and expensive to enforce at all, as well as distracting consumers from globally applicable technology likely to do a far better job.

G.3 If the whole basis of Nominet's argument is that it is practically difficult to track web sites not based in the UK, this same difficulty will prevent Nominet from adequately enforcing misuse of its trustmark by entities located abroad.

G.4 Nominet cannot scan 'domains' for infection. The best it can do is can web sites for infection. When it becomes known that Nominet scan such web sites, the infections will take countermeasures to hide from them, just as malware currently hides from search engines. Nominet would simply involve itself in a lengthy game of cat and mouse. Whilst scanning domains may well be a useful service, it is always going to have false negatives (i.e. there will always be sites which legitimately or otherwise bear the trust mark that are infected); this will reduce the value of the trust mark. Therefore if this service is offered, it should not be linked to any trust mark. Furthermore, there is no reason not to offer such a service to the remainder of registrants in other SLDs if it is offered within *.uk*.

G.5 Nominet appears to have misunderstood how DNSSEC works. Nominet can sign its own *.uk* domain, including the records delegating (say) *example.uk*. How does it propose to ensure 'mandatory' signing of the zone containing *www.example.uk* or *www.corp.example.uk* and the relevant records (note the signer can use OPTOUT).

G.6 Nominet also misses the point about DNSSEC. Of course it is important. This is presumably why Nominet offers DNSSEC signing of its existing zones. If Nominet wants to encourage DNSSEC adoption, I would suggest it simply waives the current £0.50 per two year signing charge, and ensure it is adopted everywhere.

G.7 Answers to specific questions:

1. (a) I believe the strategies proposed would be almost entirely ineffective. See http://www.alex.org.uk/nominet/directukresponse.pdf for details. (b) I do not believe Nominet should suspend domains based on 'notified infections' unless that is what the registrant has asked Nominet to do. I believe this should not be an option based on a specific domain. See http://www.alex.org.uk/nominet/directukresponse.pdf for details.

2. I believe the trust mark service would be almost entirely ineffective and may in fact be counterproductive. See http://www.alex.org.uk/nominet/directukresponse.pdf for details.

3. Whilst I support the goal of widening DNSSEC penetration, this is not the way to do it. Instead Nominet should simply waive its DNSSEC costs and sign every domain, whether in *.uk* or not.

H. Verification of registrant contact data

H.1 This section illustrates consumer ignorance: '*Interestingly, 67% also said they would expect a .uk site to conform to UK consumer law regarding security and data protection*', but perhaps in a misguided attempt to emulate King Canute, seeks to avoid education of the consumers in question and try to bring about the situation

where there misconceptions are slightly less incorrect. People expected the earth to be flat, but few people offered to flatten the earth.

H.2 Nominet states '*Our current registration policy is very open and does not include any restrictions or criteria necessitating a physical UK presence*'. Nominet ignores its own data here. Actually Nominet's current registration policy is very open **only** in *co.uk*. Another SLD, *ltd.uk* has a restrictive registration policy where the registrant must have UK contact details (as the registered office of a UK company must lie within the UK), and the consumer knows exactly who the registrant is. However, to my knowledge, there are no statistics suggesting an enhanced degree of consumer trust in *ltd.uk* registrations. Furthermore, *ltd.uk* registrations have not proved popular with registrants, representing only a tiny fraction of the *.uk* registration base. This suggests Nominet's own scheme will not work.

H.3 The second failure here is that Nominet assumes that merely ensuring there is a valid UK address for service is sufficient to enhance trust. If a Mr Joe Clarke, resident in the UK, registers '*clarkes.co.uk*', one might assume there is nothing wrong with that. If he starts selling shoes on the site, one might presume differently. However, Nominet proposes no different rules for *'clarkes.uk'* (beyond the sunrise period).

H.4 Nominet suggests that the integrity of the WHOIS database is important and that '*consumers have a right to know the contact details of those operating a commercial domain they are visiting or transacting with*'; I agree, and this is enshrined within Nominet's current WHOIS policy. If further WHOIS verification is needed, that should be applicable to all domains, not just those in *.uk*. Moreover, what evidence does Nominet have that consumers check WHOIS data as part of their interaction with a site? My suspicion is that only a tiny fraction of consumers know how to check WHOIS data. Whilst only a small number know how to check SSL certificates, this is an infinitely easier way to validate domain ownership. Nominet could issue free SSL certificates, or SSL certificates of different types depending on WHOIS validation.

H.5 The concept of verifying postal address by sending a letter sounds quaint, time consuming, and expensive. Nominet thankfully avoided sending things by letter when it dropped (around ten years ago) its certificates and reply forms. Why this particular corpse needs to be resurrected is far from obvious, and why it would be necessary to impose it on all registrants in the putative direct *.uk* even less so. Its only advantages appears to be increasing employment in the Oxford area and reviving the fortunes of Royal Mail.

H.6 If it is desirable to validate the UK presence and UK address of a registrant, there is a relatively simple solution. Nearly every UK business with which an end user wishes to deal commercially will be a limited company or LLP and thus registered at Companies House. Even if a sole trader does not have a Limited Company, it is possible to form one for about £20 online, which could simply hold the domain name concerned and otherwise be dormant. Nominet could simply enforce that if a company registration number is provided, the registrant and address details would constantly match the company's own details. This could be checked electronically, and could apply to all SLDs (not just direct registrations). It would also provide for continuing updates both in registered company name (across name changes) and address changes, rather than simply validation at time of registration. Furthermore it would ensure that domain names registered to companies that are struck off could be released appropriately. Even though this would present a small cost to any sole traders that wished to take advantage of this, it is unlikely to be larger than the incremental cost to all registrants of domain names, and would provide them with

prima-facie proof that they had some right to use a domain name in the event of a DRS dispute.

H.7 Answers to specific questions:

4. Provision of verifiable contact information is an issue orthogonal to registration within *.uk*. I do not believe the two should be linked. Verifiable address data is only one aspect of security. See http://www.alex.org.uk/nominet/directukresponse.pdf for more details.

5. (a) In respect of trading businesses, there are far more cheap, effective and quick ways to verify contact details. The proposed PIN mechanism should not be used. See http://www.alex.org.uk/nominet/directukresponse.pdf for more details. (b) The proposed PIN mechanism should not be used. See http://www.alex.org.uk/nominet/directukresponse.pdf for mode details. (c) Verification should be done on a continuous basis; this is not an option because Nominet has assumed a PIN mechanism should be used. See http://www.alex.org.uk/nominet/directukresponse.pdf for more details.

I. Third level sub-domains

I.1 This is a self-inflicted wound. Nominet is trying to make the direct *.uk* domain somehow special, and realising this causes problems, tries to restrict sales of subdomains. The whole idea of a differentiated *.uk* is flawed in my opinion. If it is to be released, make it work just like *co.uk*, and in that instance this problem will not arise. As it is the proposed solution has a number of problems, such as groups of companies, and would be painful to enforce. If an SSL certificate route were used, there would be no need for it anyway, as *fred.example.uk* (if sold) would only have an SSL certificate available for *example.uk*, whose owners (for obvious reasons) would be unwilling to publish a wildcard certificate. Furthermore buyers would realise that their domain name would be dependent on the continued renewal and cooperation of *example.uk*. Recent experiences with other registries dependent upon such registrations suggest that *caveat emptor* is an effective strategy.

I.2 Answers to specific questions:

6. No, I do not agree with the prevention of sale of sub-domains to third parties. The only rationale for it is as a consequence of other policies with which I disagree. Even if those were implemented, it would be unnecessary. See http://www.alex.org.uk/nominet/directukresponse.pdf for more details.

J. Reserved And Protected Names

J.1 The proposed policy in practice prevents further SLDs being registered. For instance, if a new corporate body (say an LLC) were introduced, it is unlikely Nominet would be able to introduce *llc.uk*. If direct registrations within *.uk* had the same registration policy as *.uk*, this strategy would probably be acceptable. However, if the proposed policies were adopted, there will no doubt continue to be demand for some SLDs, and for this reason it is suggested that were the proposed policy adopted, all names of 3 or fewer letters be reserved.

J.2 Answers to specific questions:

7. (a) No. (b) If the registration policies in *.uk* matched those in *.co.uk* then I would agree. If not, then I believe all domains with 3 letters or fewer should be reserved for future SLDs. See http://www.alex.org.uk/nominet/directukresponse.pdf for more details.

K. Phased Release and Rights Management

K.1 It should be emphasised that this another self-inflicted problem. Firstly, no phased release or rights management problem would arise if Nominet did not open up *.uk*. Secondly, the obvious solution is to automatically register, free for a period of time the *.uk* domain name corresponding to each *.co.uk* domain name; this is only not available as a solution because Nominet proposes adopting a peculiar set of registrations rules.

K.2 It is proposed to follow a sunrise test similar to that done for two letter domain names. This was hardly rigorous in terms of threshold test for IPR judging by some of the results.

K.3 It is not evident to me why a holder of '*example.co.uk*' that possesses unregistered rights and may have been trading in the UK for many years should have his rights to '*example.uk*' subordinated to (for instance) the holder of a non-UK recently registered trademark. Neither is it evident why a longstanding holder of '*example.co.uk'* with a UK registered trademark should have to bid at auction against a recent non-UK registrar or a similar trademark. This appears to be a convenient money making exercise for Nominet (and/or those organisations to which it dispenses its surplus).

K.4 An alternate process would be to allocate the rights in all *.uk* names to be released that correspond with a *.co.uk* name firstly to the registrant of that *.co.uk* name. The registrant would need to show that it could meet the registration requirement within *.uk* (whatever those registration requirements might be), and if these were not met, the process suggested would be followed. For a period of a month after registrations would be permitted, no records would be delegated. During this period, any person claiming to have a right to the name could make a DRS challenge using the normal rules, save that if a predecessor *co.uk* name existed, the time of registration would be deemed to be the time of registration of the *co.uk* name. At the termination of the period of a month, only those names not under a current challenge would have delegations added.

K.5 I do not agree with the need for rights protection for expired domains. If there is a need for this, it should apply to all SLDs. No cogent reasoning is presented for this applying just to *.uk*. Most of these would be better solved with a wait list than an auction, which might or might not have protection for IPR holders.

K.6 Answers to specific questions:

8. (a) No. (b) No. (c) Yes. (d) Yes. Further comments: Priority should be given to existing *.co.uk* applicants who are capable of meeting the registration criteria. See http://www.alex.org.uk/nominet/directukresponse.pdf for more details.

L. Channel to Market

L.1 This proposal is poorly thought out. Nominet is intending to verify the data itself, by sending a PIN through the post. If it does that (or uses a more efficient mechanism), further verification by the registrar should be unnecessary. However, to the extent that mandating registrar behaviour is necessary, this should be done through the normal registrar agreement, by requiring that the registration data conforms with the appropriate rules for the zone in which the domain name is registered. If the registrar does not perform, sanctions should be taken, and ultimately the registrar agreement should be terminated. There is no need for a 'two-tier' structure.

L.2 Answers to specific questions:

9. (a) No. (b) An obligation for the registrar to provide the correct data should be built into the registrar agreement (indeed is already there) and this contractual term should be enforced. A two tier registrar arrangement is unnecessary.

M. Existing Second Level Domains

M.1 Comments given as answers to specific questions:

10. (a) This proposed approach does **not** indicate a full commitment to support the existing SLDs. It instead creates 'second class citizen' registrations which Nominet will through its marketing imply are less secure, safe and trustworthy than domains registered directly within *.uk*. It will also create shorter domains, which are perceived to be more attractive. This will put pressure on existing registrants to register the *.uk* equivalents if they are permitted (which is inevitable if *.uk* is to be opened), but also pressure to rebrand away from the 'insecure' existing SLD names (which is not inevitable) and incur the large costs associated therewith. For those unlucky registrants who cannot reregister within *.uk* (possibly as a competing trademark holder outbids them), they will be consigned to be the holder of only 'the insecure name'. As such, and as structured, the proposal is deeply unfair. I do not hold a portfolio of names that will be affected by this change (the main domain I use is an *org.uk*) so have no personal Axe to grind. See http://www.alex.org.uk/nominet/directukresponse.pdf for more details. (b) Yes.

N. General views

N.1 Comments given as answers to specific questions:

11. (a) Not under any circumstances. Further comments: The proposal to open up *.uk* and to introduce additional security are worth considering, but are separate issues and this paper is so flawed the matter should be revisited from scratch (b) Yes. See http://www.alex.org.uk/nominet/directukresponse.pdf for more details. (c) Yes. Any and all security features introduced should be introduced to all domains managed by Nominet. See http://www.alex.org.uk/nominet/directukresponse.pdf for more details.