Operating nidirect.gov.uk  
 sub domains [DRAFT v1.1]

Department of Finance and Personnel

September 2013

Contents

[Introduction 3](#_Toc361739843)

[One entry point 3](#_Toc361739844)

[Creating a domain 3](#_Toc361739845)

[Sub domains 4](#_Toc361739846)

[Maximum number of visible sub domains 4](#_Toc361739847)

[Usernames and passwords 4](#_Toc361739848)

[Multiple environments 5](#_Toc361739849)

[Transport Layer Security 5](#_Toc361739850)

[Cookies 5](#_Toc361739851)

[robots.txt and root level redirections 6](#_Toc361739852)

[Emails sent to service users 6](#_Toc361739853)

# Introduction

nidirect.gov.uk offers a number of different digital services to citizens. While the start and end of a user’s journey will be on [www.nidirect.gov.uk](http://www.nidirect.gov.uk), the service itself will typically be hosted elsewhere, and will need a different domain name as a result. This document describes the use of nidirect.gov.uk sub domains for hosting digital services.

**Note:** This document is written as a ‘standard’, and as such uses the words MUST, SHOULD, MAY and MUST NOT as defined in [RFC 2119](http://www.ietf.org/rfc/rfc2119.txt).

# One entry point

The user journey for every digital service offered by nidirect MUST begin on a relevant start page on [www.nidirect.gov.uk](http://www.nidirect.gov.uk) – for instance, the Benefit Adviser service start page is at <http://www.nidirect.gov.uk/benefits-adviser>.

Service managers MUST NOT advertise any URL other than that of the start page as the entry point for the relevant service. This is what gets printed on literature and used in email signatures, advertising, press releases and any other forms of communication.

The start page URL for a given service will be allocated by nidirect’s Central Editorial Team based on discussions with the service manager and analysis of user behaviour, search referrals and other relevant data.

# Creating a domain

The transactional part of a service – the dynamically generated pages where users interact with the service – will typically not be hosted on the nidirect.gov.uk domain. That means that each service (or group of services) will require its own domain name for the transactional part of the service(s).

**Note:** This does not apply to interactive tools on the nidirect.gov.uk domain which are developed and maintained by ESS (Enterprise Shared Services) in partnership with other NI government departments.

For all new digital services offered by nidirect (going live from 1 April 2013), ESS will create a fourth level domain name of the form **servicename.**nidirect.gov.uk where “servicename” is a plain English description of the service(s) agreed between the relevant dept/agency, nidirect’s Central Editorial Team, and ESS. This will introduce consistency across NI central government domains for citizen-facing digital services and remove the dependency on departmental sub domains (which are of course vulnerable to machinery of government changes).

The process of obtaining an nidirect.gov.uk sub domain begins when the service owning dept/agency has engaged with the nidirect Central Editorial Team / ESS prior to application development or when the service manager asks an nidirect theme manager for a start page on nidirect.

Sub domains of nidirect.gov.uk SHOULD describe the service (e.g. reportafault.nidirect.gov.uk).

Sub domains SHOULD NOT contain:

* the name or abbreviated name of the service owning department or agency
* the two letter abbreviation for Northern Ireland

The service-owning dept/agency will be given delegated authority to manage the sub domain (and its sub domains) in association with ITAssist and third party suppliers. The service-owning dept/agency will at all times remain responsible for ensuring the standards presented here are adhered to.

# Sub domains

This section gives some guidance about which sub domains a service manager should create once they have been given control of servicename.nidirect.gov.uk.

## Maximum number of visible sub domains

The user-facing live service SHOULD be operated using at most two user-visible sub domains of servicename.nidirect.gov.uk:

1. assets.servicename.nidirect.gov.uk is for assets such as static images and shared javascript files needed to run your live service. Note: written content about the service, such as guides to eligibility or detailed guidance for applicants, MUST be placed on [www.nidirect.gov.uk](http://www.nidirect.gov.uk) and not duplicated on a sub domain.
2. admin.servicename.nidirect.gov.uk is for features that enable non-technical staff to run the service (e.g. contact centre staff might use this sub domain to access and process work items where human judgement is needed).

You SHOULD NOT create separate domains for APIs unless there is a really good reason to have a completely separate domain.

Service managers should notify the ESS Web and Design Team or nidirect’s Central Editorial Team if you intend to create user-visible sub domains other than the two listed above. We are happy to discuss exceptions and edge cases.

## Usernames and passwords

If the service is a private alpha or private beta release then it should be protected by a username and password known only to the development team and the users who are testing the service. If a service, or part of a service, is a public alpha or beta release, then it should be clearly marked as such with a text label (i.e. not an image containing the word alpha or beta) on every page and in every API response.

## Multiple environments

It is good practice to have multiple ‘environments’ for the development, testing and live (aka production) versions of any service. The development and testing environments allow the team to assess the correctness and quality of the service before it goes live. Typically, the sub domains used to access a development or testing instance of the service are structured in the same way as the sub domains used in the live version of the service.

Therefore, you MAY create other sub domains of servicename.nidirect.gov.uk for use in testing and development, such as preview.servicename.nidirect.gov.uk and dev.servicename.nidirect.gov.uk. If there is a compelling reason to use a non .gov.uk domain for testing and/or development sub domains, that is also acceptable.

Regardless of the domain name used, web-based services on testing and development domains (including APIs) should be protected by a username and password along the same lines as private alpha and beta releases.

# Transport Layer Security

Many services will collect personal and/or sensitive information from users. It is essential that this information cannot be intercepted by malicious third parties as it travels over the Internet.

Therefore, all services that collect personal or sensitive information accessed through nidirect.gov.uk domains (including APIs) MUST only be accessible through secure connections. For web-based services this means HTTPS only (often referred to by the acronyms TLS or SSL, which both refer to the protocol underpinning these secure connections). Services that collect personal or sensitive information MUST NOT accept HTTP connections under any circumstances.

Once a service manager has verified that their HTTPS setup is working correctly they SHOULD enable HSTS (HTTP Strict Transport Security) on the production domains (admin. and assets.), by setting an HTTP response header such as:

Strict-Transport-Security: max-age=1209600, includeSub domains;

This represents a commitment to HTTPS-only traffic for 14 days. Once the service manager is confident that HSTS is configured correctly, you SHOULD increase the commitment to months or years:

Strict-Transport-Security: max-age=31536000, includeSub domains;

# Cookies

Cookies MUST be scoped to the originating domain only. For instance, if the cookie originates from admin.servicename.nidirect.gov.uk the cookie MUST NOT be scoped to servicename.nidirect.gov.uk.

Cookies SHOULD NOT be used on assets.servicename.nidirect.gov.uk (they introduce a browser overhead that slows down the response time for users without providing any benefit for the service manager).

For services using HTTPS, cookies MUST be sent with the Secure attribute and SHOULD, where appropriate, be sent with the HttpOnly attribute. These flags provide additional assurances about how cookies will be handled by browsers.

# robots.txt and root level redirections

nidirect.gov.uk is the place for users to find all government services, so it is essential to ensure that users always start on the relevant nidirect.gov.uk page, rather than a different or duplicate start page on servicename.nidirect.gov.uk.

As a result, services need to ask search engines not to index pages on their domains, so that the relevant nidirect.gov.uk page and the service domain do not compete with each other in search engine results. This can be achieved by redirecting users to the relevant nidirect.gov.uk start page if they go directly to the service’s domain name, and by asking search engines not to index pages on the service’s domain name. Therefore, every service hosted on an nidirect.gov.uk sub domain MUST:

* Have a robots.txt file asking search engines not to index any part of the site. Example content for robots.txt is given below, and more details can be found on [The Web Robots Pages](http://www.robotstxt.org/):  
    
  User-agent: \*  
  Disallow: /
* Have an HTTP 301 redirection from the top-level index page of the sub domain to the relevant start page on nidirect.gov.uk. (Note: this means that the service start page on nidirect.gov.uk SHOULD NOT link to the root of the service sub domain.)

# Emails sent to service users

Emails to users of your service SHOULD be sent from a human-monitored email address that originates from the domain servicename.nidirect.gov.uk (and not the dept/agency or any other domain name).

You SHOULD enable [SPF](http://en.wikipedia.org/wiki/Sender_Policy_Framework) (Sender Policy Framework) on the sending domain. You MAY also want to use [DKIM](http://www.dkim.org/) (DomainKeys Identified Mail) on the sending domain; it can provide additional guarantees about message delivery and help recipients to more easily distinguish genuine mail from forgery.