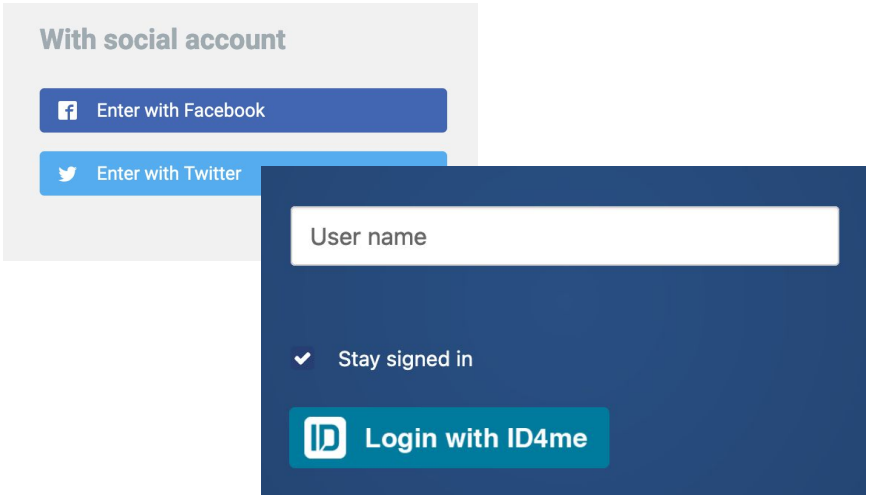
Using the Registrant Email Address Field to connect Identity Services to Domain Names



ROW#10
June 8th, 2021
Werner Staub
CORE Association
werner.staub@corenic.org

core Internet Council of Registrars

GAISF Global Association of International Sports Federations

.SPORT

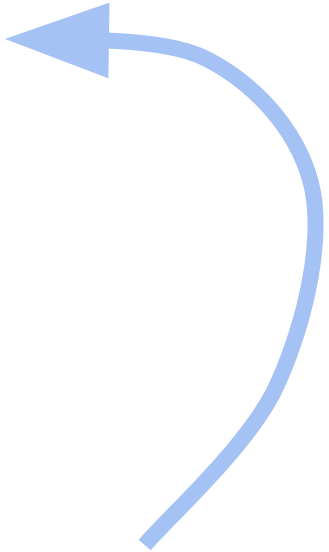
kalashnikov.sport	domains@kalashnikov.ru
kalashnikov.sport	info@kalashnikov.sport
kalashnikov.sport	Elena.Mikhailova@kalashnikov.sport
kalashnikov.sport	accounts@xyzstudio.ru
kalashnikov.sport	xyzstudio@gmail.com
kalashnikov.sport	56hi8a8s4gh@relay.apple.com
kalashnikov.sport	kalashnikov.sport@privacyclub.xyz

Imagine the various possibilities of a domain registered with the email address next to it as shown above...

kalashnikov.sport	**domains@kalashnikov.com**
kalashnikov.sport	info@kalashnikov.sport
kalashnikov.sport	Elena.Mikhailova@kalashnikov.sport
kalashnikov.sport	accounts@xyzstudio.ru
kalashnikov.sport	xyzstudio@gmail.com
kalashnikov.sport	56hi8a8s4gh@relay.apple.com
kalashnikov.sport	kalashnikov.sport@privacyclub.xyz

Establishes link to pre-existing brand. But this quality cannot be inferred by machine.

kalashnikov.sport	domains@kalashnikov.com
kalashnikov.sport	**info@kalashnikov.sport**
kalashnikov.sport	Elena.Mikhailova@kalashnikov.sport
kalashnikov.sport	accounts@xyzstudio.ru
kalashnikov.sport	xyzstudio@gmail.com
kalashnikov.sport	56hi8a8s4gh@relay.apple.com
kalashnikov.sport	kalashnikov.sport@privacyclub.xyz



Will fail if domain fails. Cannot be used as proof of authority for initial registration.

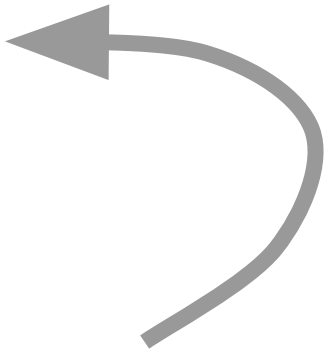
kalashnikov.sport	domains@kalashnikov.com
kalashnikov.sport	info@kalashnikov.sport
kalashnikov.sport	**Elena.Mikhailova@kalashnikov.sport**
kalashnikov.sport	accounts@xyzstudio.ru
kalashnikov.sport	xyzstudio@gmail.com
kalashnikov.sport	56hi8a8s4gh@relay.apple.com
kalashnikov.sport	kalashnikov.sport@privacyclub.xyz

Creates added concern about private data as it refers to a natural person. Machines are unable to tell personal email addresses from role-based ones.

kalashnikov.sport	domains@kalashnikov.com
kalashnikov.sport	info@kalashnikov.sport
kalashnikov.sport	Elena.Mikhailova@kalashnikov.sport
kalashnikov.sport	**accounts@xyzstudio.ru**
kalashnikov.sport	xyzstudio@gmail.com
kalashnikov.sport	56hi8a8s4gh@relay.apple.com
kalashnikov.sport	kalashnikov.sport@privacyclub.xyz

Involves professional intermediary (PR firm / Ad agency) whose role cannot be verified or inferred by machine

kalashnikov.sport	domains@kalashnikov.com
kalashnikov.sport	info@kalashnikov.sport
kalashnikov.sport	Elena.Mikhailova@kalashnikov.sport
kalashnikov.sport	accounts@xyzstudio.ru
kalashnikov.sport	**xyzstudio@gmail.com**
kalashnikov.sport	56hi8a8s4gh@relay.apple.com
kalashnikov.sport	kalashnikov.sport@privacyclub.xyz

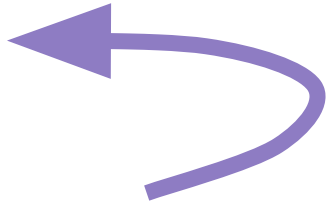


Anybody could have created this email address.

kalashnikov.sport	domains@kalashnikov.com
kalashnikov.sport	info@kalashnikov.sport
kalashnikov.sport	Elena.Mikhailova@kalashnikov.sport
kalashnikov.sport	accounts@xyzstudio.ru
kalashnikov.sport	xyzstudio@gmail.com
kalashnikov.sport	**56hi8a8s4gh@relay.apple.com**
kalashnikov.sport	kalashnikov.sport@privacyclub.xyz

Offers enhanced identity management capabilities only if integrated by implementing a proprietary protocol

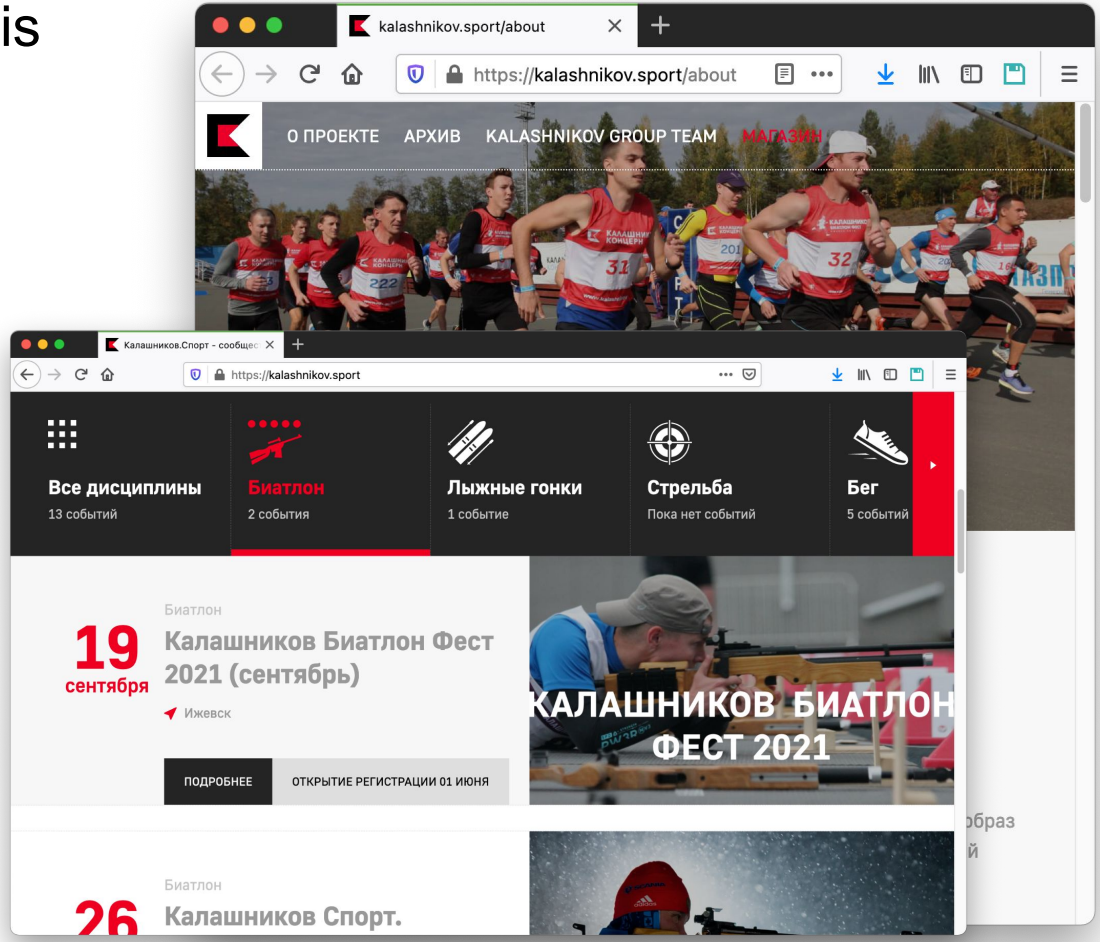
kalashnikov.sport	domains@kalashnikov.com
kalashnikov.sport	info@kalashnikov.sport
kalashnikov.sport	Elena.Mikhailova@kalashnikov.sport
kalashnikov.sport	accounts@xyzstudio.ru
kalashnikov.sport	xyzstudio@gmail.com
kalashnikov.sport	56hi8a8s4gh@relay.apple.com
kalashnikov.sport	**kalashnikov.sport@privacyclub.xyz**



Would trigger rejection of domain registration by the .sport registry's validation team. Other registries accept such email addresses but create a danger to the public in doing so.

N.B. Actual Site and Whois

Domain Name: **kalashnikov.sport**
Registry Domain ID: **Disjr9041-SPORT**
Registrar WHOIS Server:
Registrar URL: **https://www.nic.ru/en/**
Updated Date: **2021-01-28T09:01:16.671Z**
Creation Date: **2019-01-24T18:04:11.844Z**
Registry Expiry Date: **2022-01-29T18:42:26.633Z**
Registrar Registration Expiration Date:
Registrar: **RU-CENTER**
Registrar IANA ID: **463**
Registrar Abuse Contact Email: **tld-abuse@nic.ru**
Registrar Abuse Contact Phone: **+7.4957377664**
Reseller:
Domain Status: **clientTransferProhibited**
https://icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name:
Registrant Organization: **Obshchestvo s ogranichennoy otvetstvennostu "KALAShNIKOV SPORT"**
Registrant Street:
Registrant City:
Registrant State/Province: **Udmurtiia**
Registrant Postal Code:
Registrant Country: **RU**
Registrant Phone:
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: **Please query the Whois service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.**



More imaginary examples, this time for a natural person

heidihofer.sport	heidihofer@gmail.com
heidihofer.sport	privacy@privacyclub.xyz
heidihofer.sport	k98k56kcfua44@id.gandi.net
heidihofer.sport	67b3g5@id.sport
heidihofer.sport	67b3g5@67b3g5.id.sport

Email address **not** for receiving email?

Proposed approach

A TLD registry has Accredited Identity **Schemas**.

For instance, .sport accredits id.sport and id.music . Each identity schema can be recognized by the suffix on the right of the @ sign.

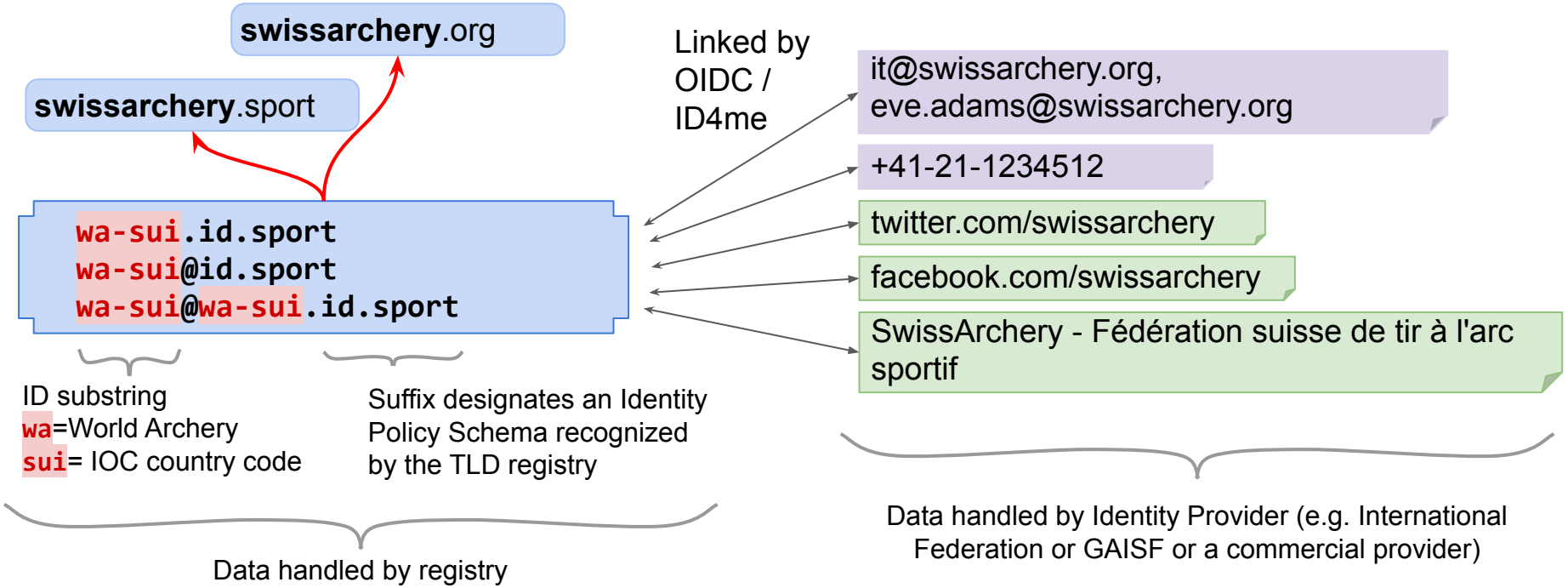
Each Accredited Identity Schema has accredited Identity **Providers**.

Data subjects can transfer the identifiers between accredited identity providers in the same way as domain holders can transfer domains between registrars.

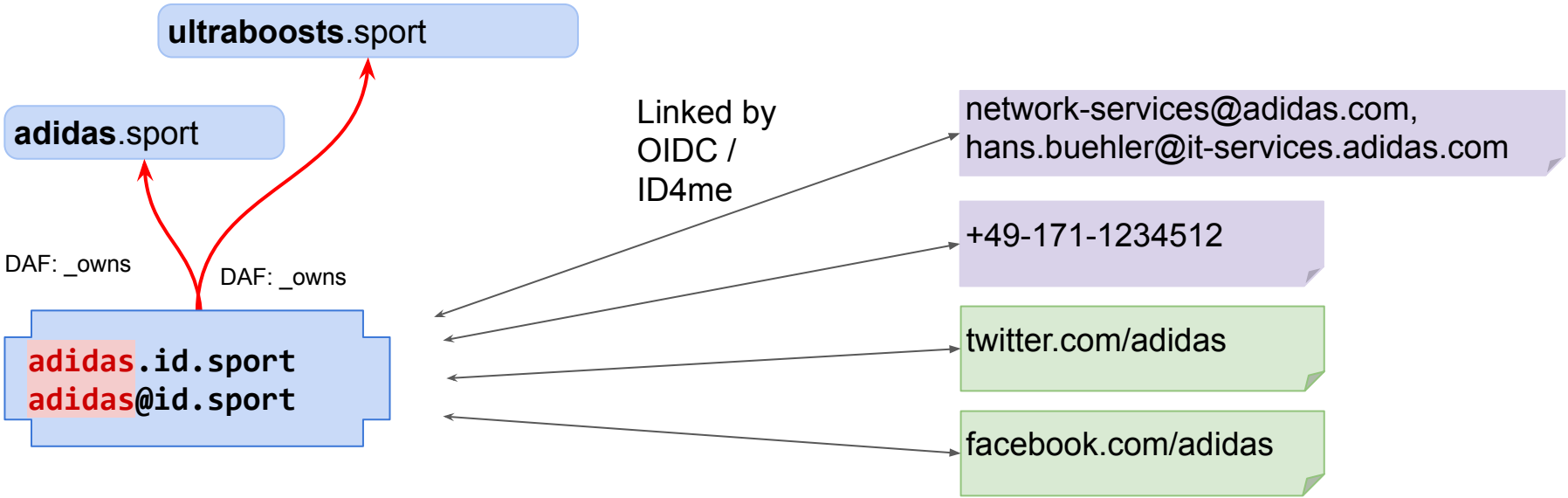
Registrant email strings with identity schema suffix are **published** on Whois/RDDS/RDAP.

The identity schema policies prevent leakage of private data. Message receipt may be restricted to trusted notifiers and may exclude or limit SMTP.

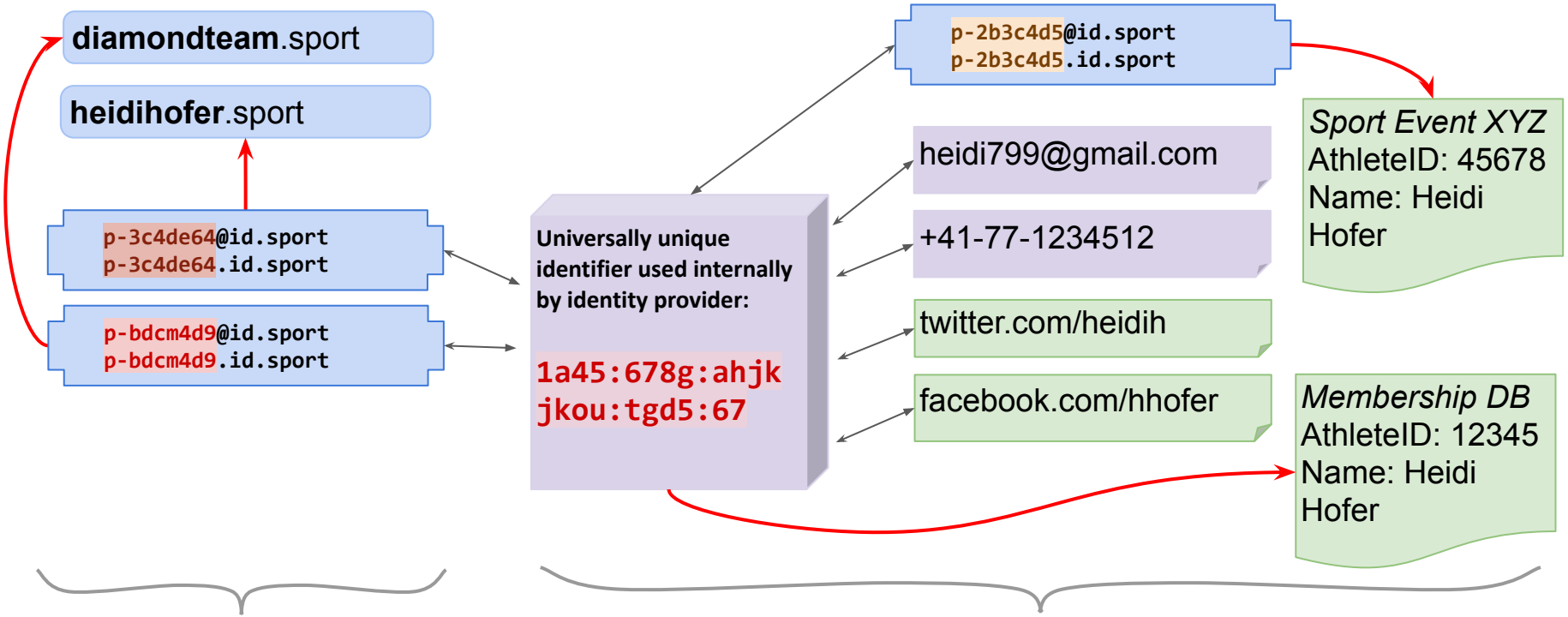
Example: **Identifier** for a national sport federation



Identifier for a brand in email field



Natural or persons: 1 identifier per relationship



How is identifier portability achieved?

wa-sui.id.sport
wa-sui@id.sport
wa-sui@wa-sui.id.sport

All variants identify same party

The policy of the identity schema (**id.sport** in the example above) defines that the @ sign may be replaced by a dot, and that the identifying substring (**wa-sui** above) may be repeated before and after the @ sign.

In this way, at least one form of the identifiers (**wa-sui.id.sport** above) can be delegated in the DNS to an accredited provider of the data subject's choosing. The data subject can thus change identity provider without having to replace the identifiers stored in registries or other systems.

```
Authorization
0a.  (N)ew (M)odify (D)elete....:
0b.  Auth Scheme................:
0c.  Auth Info..................:

1.   Comments..................:

2.   Complete Domain Name.......:

Organization Using Domain Name

3a.  Organization Name..........:
3b.  Street Address.............:
3c.  City.......................:
3d.  State......................:
3e.  Postal Code................:
3f.  Country....................:

Administrative Contact
4a.  NIC Handle (if known)......: WS67
4b.  (I)ndividual (R)ole........:
4c.  Name (Last, First).........:
4d.  Organization Name..........:
4e.  Street Address.............:
4f.  City.......................:
4g.  State......................:
4h.  Postal Code................:
4i.  Country....................:
4j.  Phone Number...............:
4k.  Fax Number.................:
4l.  E-Mailbox..................:
```

In an era of many registries, portable identifiers are a way to bring back the advantage of the "NIC Handle" of yore, when a given party could use the same identifier all the time, as in this Internic email registration template of 1998

Summary of Rationale

Why use the Email field?	The email field exists in all data models for domain registrations. Existing RDDS/Whois/RDAP lookup resources support it. Users have learned to equate email address with identity. Email suffix can designate identity provider policy (identity schema).	
Why Identity Services?	Domain's holder identity must be the **means of control** over the domain.	
	Why that?	To protect the registrant (domain portability) To protect the public (registrant accountability)
Why not just standard email?	Unfiltered receipt of email is dangerous (spam, phishing). Objectives are identity, control and notifications (in that order). Email has never been designed for that. A natural person's normal email address should not be in domain registry.	
Why portable identifiers?	To avoid forcing the domain holder to hand over private identifiers multiple parties. To avoid a proliferation of badly managed contact records.	