

Privacy/Proxy Accreditation Program: Potential Framework Models Comparison

	Contract/Policy Model ("Registrar Model")	Sponsorship/Contract Review Model ("Third Party Provider/Data Escrow Model")	Pass-Through Model ("Reseller" Model)	Policy + Rules Model ("UDRP" Model)
Accreditation Process	Privacy/proxy service submits accreditation application to ICANN. Service is screened and (if it meets screening criteria) accredited by ICANN.	Privacy/proxy service applies for accreditation/approval to ICANN, and must declare a relationship with registrar(s) as a condition of approval.	Requirements for privacy/proxy services passed down automatically via services' agreements with ICANN-accredited registrars (via requirements in the RAA). ICANN is not involved in the screening of these services.	ICANN approves service provider based on defined criteria. Each service provider has its own set of supplemental rules (which cannot be contrary to the UDRP and cover topics such as fees, technical requirements for communicating with the service provider, etc). ICANN reviews supplemental rules to confirm there is no conflict with UDRP rules or Policy. ICANN's relationship with URS providers is distinct from the UDRP provider relationship because, instead, there is a Memoranda of Understanding, in which URS providers agree to implement the URS services in accordance with the procedures laid out in the Applicant Guidebook. URS providers also agree to maintain supplemental rules that may not contravene or be inconsistent with the URS Procedure or the URS Rules.
Contractual Structure	ICANN would enter into Accreditation Agreement with Privacy/Proxy service for a defined period. Standard (non-modifiable) Accreditation Agreement terms would likely be generated from Policy requirements and additional necessary terms and conditions.	ICANN would screen/approve agreement between Privacy/Proxy service and registrar. In addition, ICANN might or might not be a party to that agreement or a third-party beneficiary.	ICANN does not enter into contract with privacy/proxy service. All contractual requirements are placed on registrars to be passed down in agreements with registrants who provide privacy/proxy services.	ICANN would approve privacy/proxy service provider based on defined criteria. Each privacy/proxy service could have its own set of supplemental rules (which could not be contrary to Policy).
Enforcement Mechanism(s)	ICANN Compliance would manage enforcement and respond to complaints, as required.	Enforcement mechanism would depend on whether or not ICANN was a party to the contract (though it is unlikely that enforcement would be managed directly by ICANN Compliance). ICANN would have the option to terminate approval of provider if they are not following requirements.	Compliance-related enforcement through registrar via RAA.	ICANN could rescind approval of service provider, but no Compliance enforcement mechanism.