Designing a Better Registration System for Registries, Registrars and Requesters

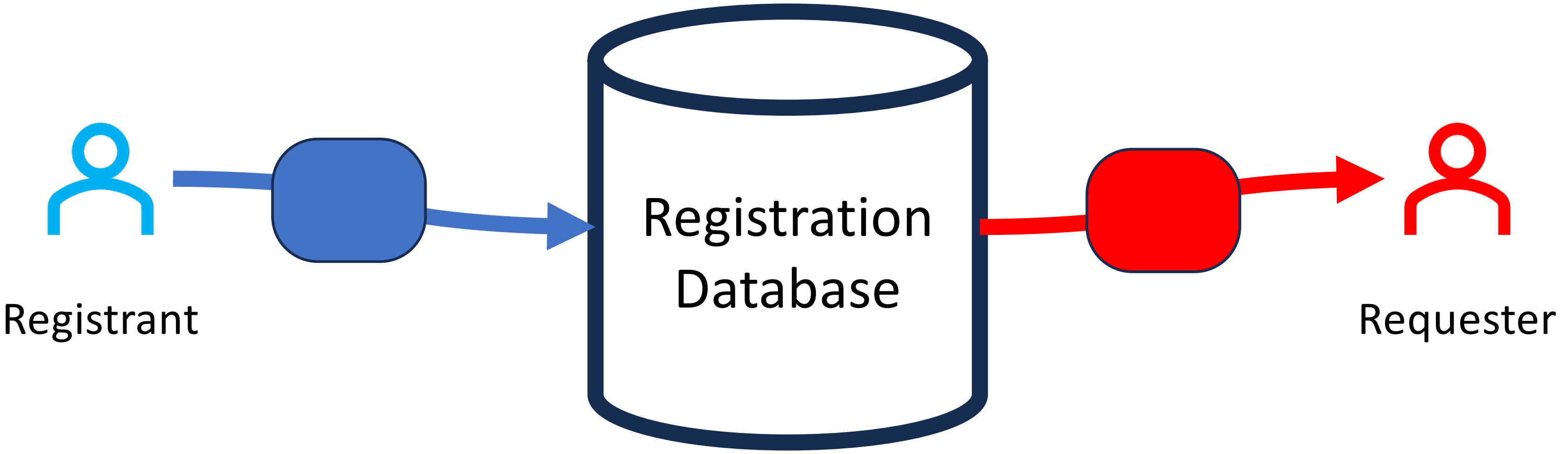
Presentation at ROW12

20 June 2023

Steve Crocker, Edgemoor Research Institute

steve@shinkuro.com

Collections and Requests



Need to Design Both Sides Together

Access, Protection, Efficiency

- Requesters want/need access to registration data
  - Variable levels of access
- Registrants need protection against abuse
  - Some need more protection than others
- Registrars need legal protection
- Everyone needs efficiency
  - Efficiency reduces costs
  - Efficiency improves effectiveness

Observations

- Registration Data includes a LOT of data elements
  - Contacts
  - DNS records
  - Payment details
  - Account Holder
  - Locks, etc.
- Everybody has policies
  - Registrars, Registries, Policy Authorities
  - Need to fit them together

Design Approach

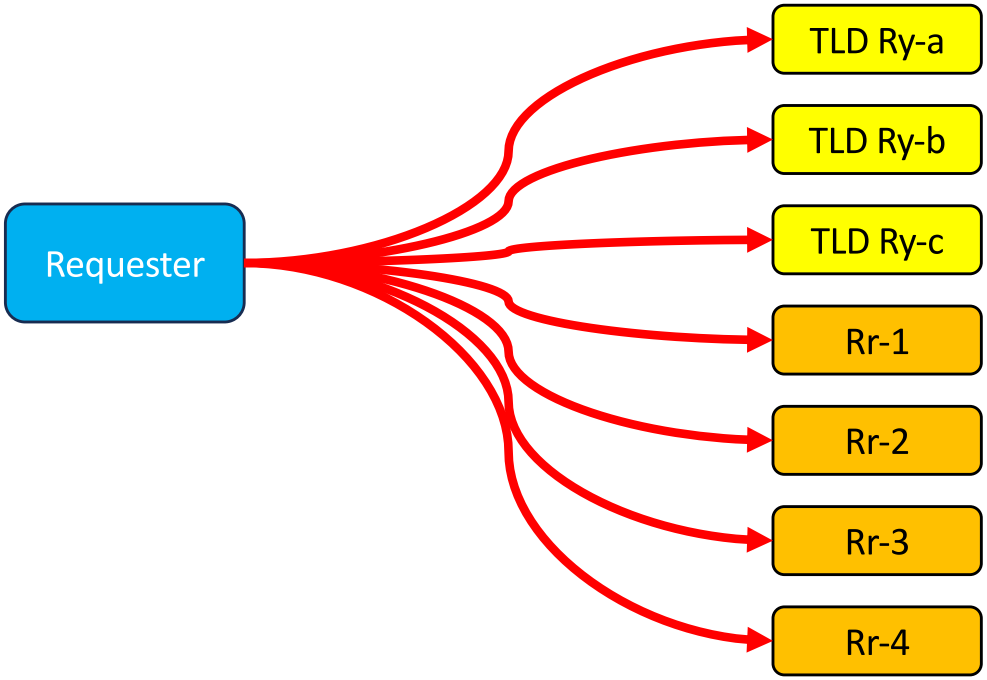
- Assign validation and sensitivity levels
  - to each data element
- Might be dependent on the registrant’s status
  - PII, At risk, etc.
- Use a two-dimensional filter on requests
  - Permitted Sensitivity Level
  - Permitted Data Elements

Policy controls are via assignments of sensitivity levels and control of who is permitted to see which data elements.

The Requester’s View

Requester’s ideal:

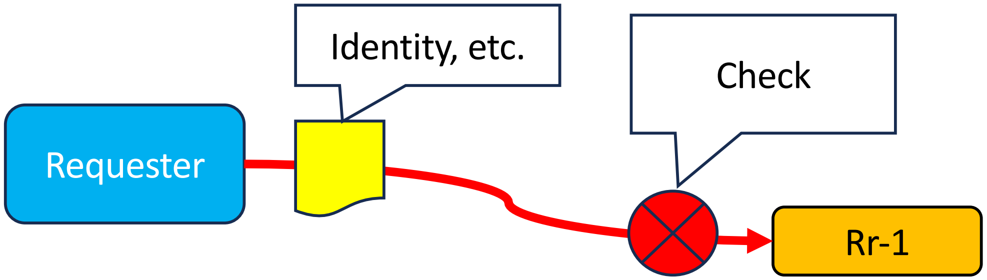
- Ask anybody for anything
- Ask everybody for everything



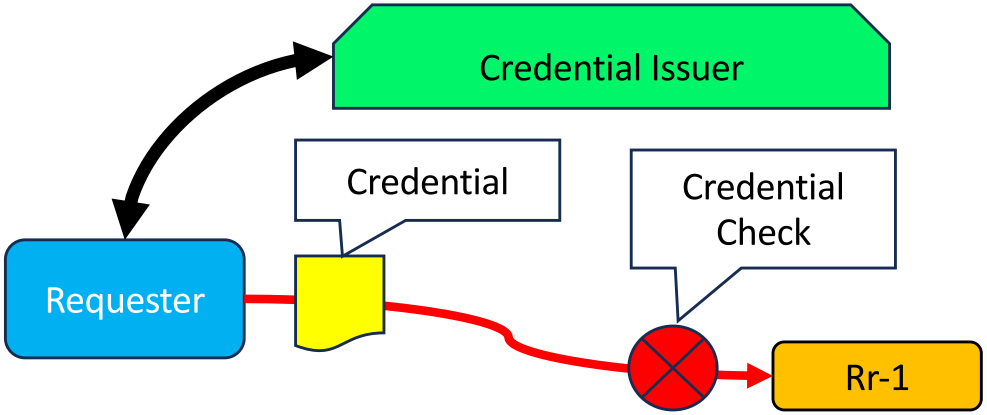
Reality check: GDPR, et al

- Need to protect privacy, prevent abuse
- Variable access
  - Who/why
  - What data
- Need identification, authentication and authorization
  - Credentials ahead of time for efficiency and certainty
  - Ad hoc requests also ok, but triggers manual review

New reality: Who?, Why?, What data?



Pre-authorization speedup



Credentials

- Identity of requester
- Terms
    - Purposes
    - Protection of data
    - Audit, Enforcement

- Acceptance
    - Bilateral
    - Specific groups
    - Broad groups

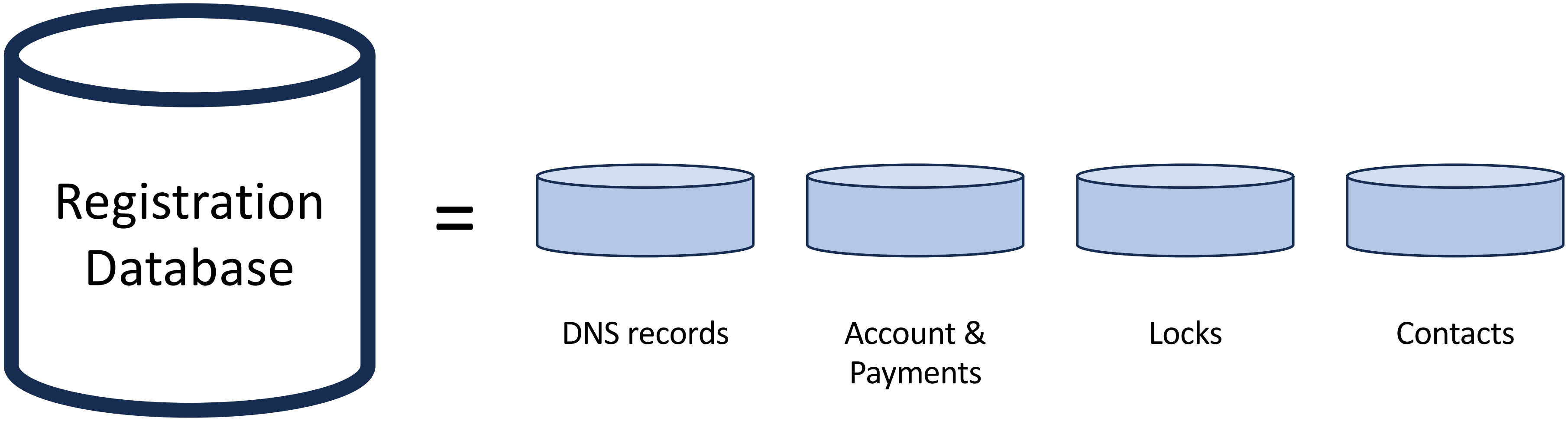
Credential Acceptance

	Rr group 1	Rr group 2	Rr group 3	Rr group 4
LE-1	✓	✓		✓
LE-2	✓	✓	✓	
IP		✓		
Sec Prac	✓		✓	

These all evolve over time

- Requester groups admit and oversee members
- Registrars and Registries join various groups
- Groups arise, merge and fade

The Hierarchy



Registration Database

=

DNS records

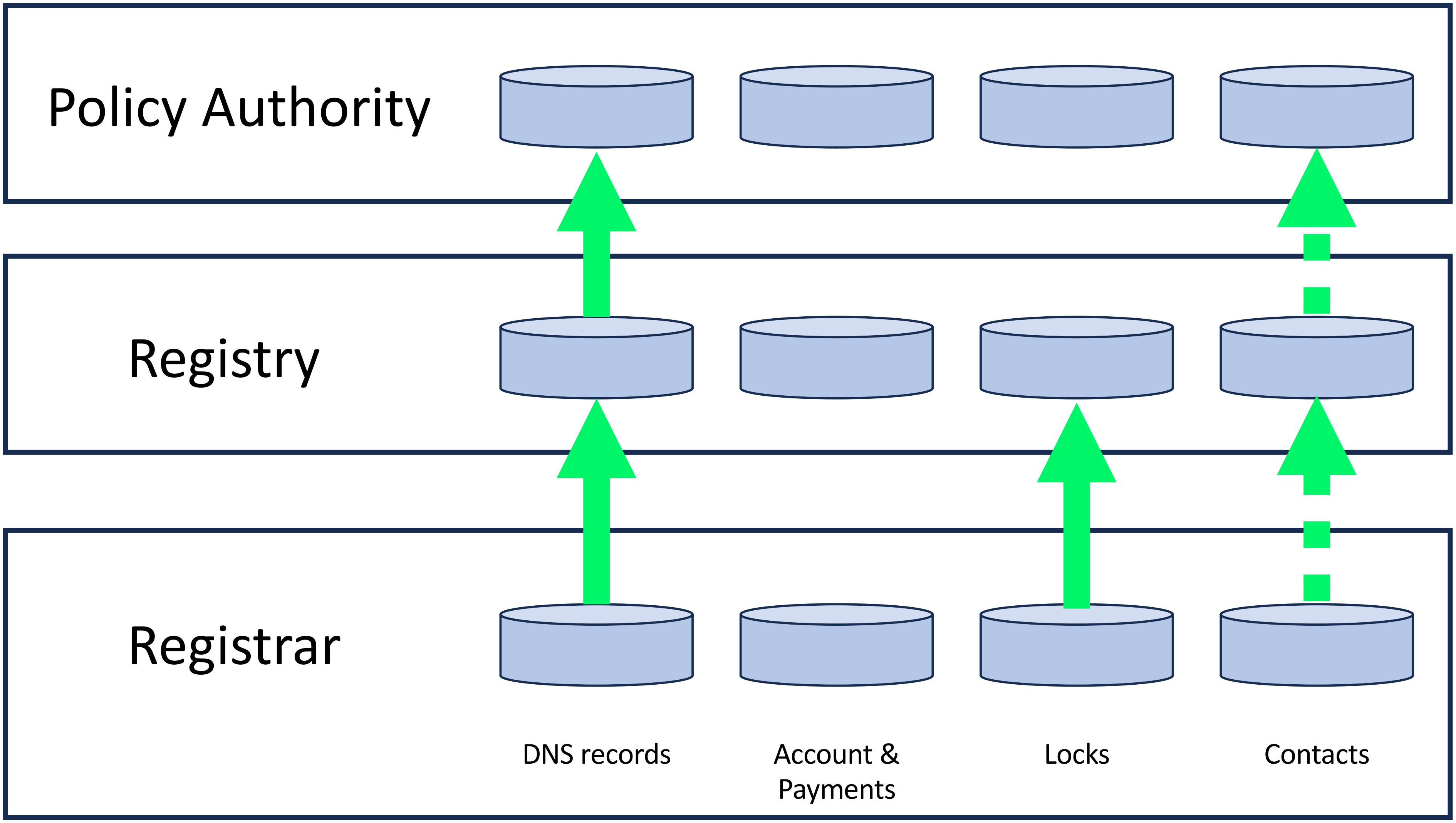
Account & Payments

Locks

Contacts

Multiple Policy Levels

- Registrar has one or more policies regarding
  - What data to collect
  - Validation process
  - Assignment of sensitivity level
- Registries also have policies
- And Governments, ICANN, et al do too (Policy Authorities)


Policy Authority
Registry
Registrar
DNS records
Account &
Payments
Locks
Contacts

Collection, Validation and Labelling

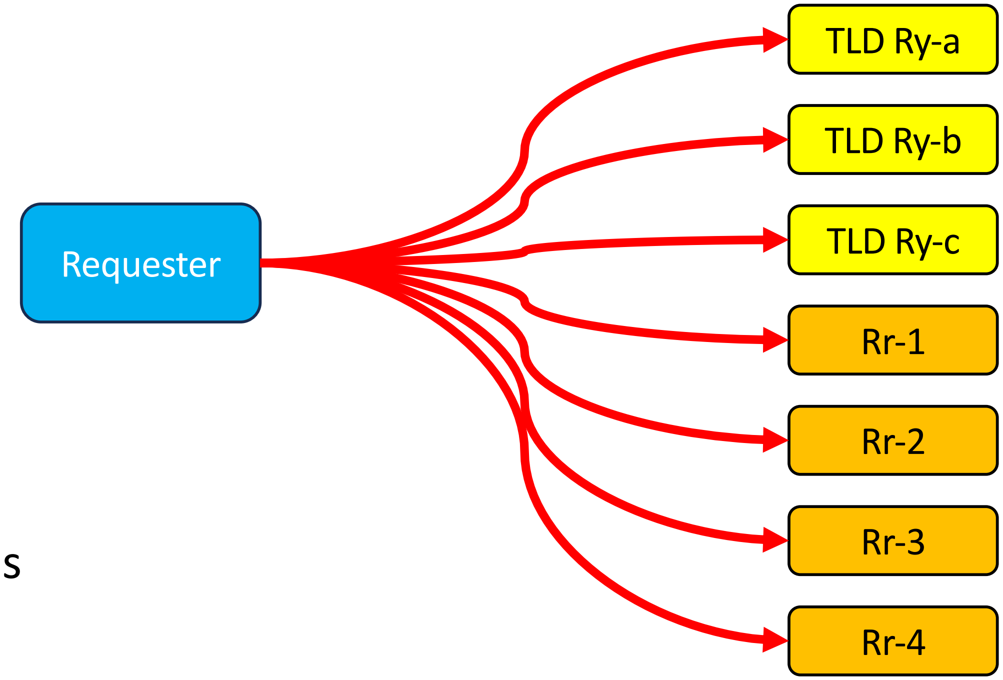
- What data must/may be collected?
- Validation of each data element?
    - V0 = no validation
    - V1 = syntactic validation
    - V2 = operational validation
    - V3 = identity validation

- Sensitivity Levels
    - S0 = public
    - S1 = private
    - S2 = very private
    - S3 = requires legal paperwork
- Who gets a copy?
    - Registrar (of course)
    - Registry
    - Policy Authority (ICANN, Gov, etc.)

Search and Summary

Requester's ideal:

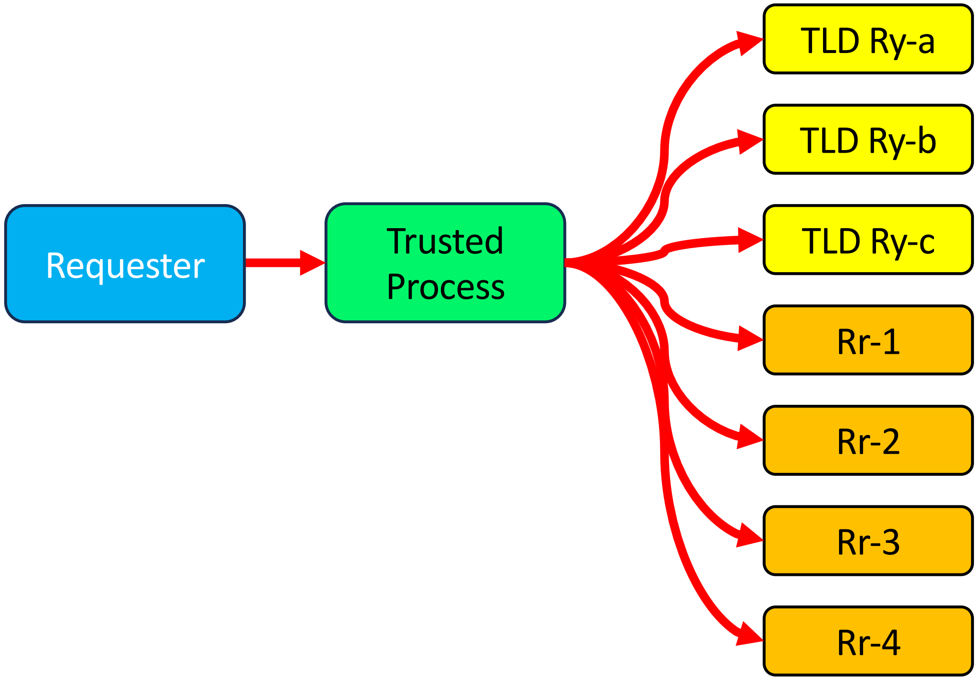
- Ask anybody for anything
- Ask everybody for everything
- Correlate and Summarize as desired



However:

- Need to limit and audit this process

Trusted Processes

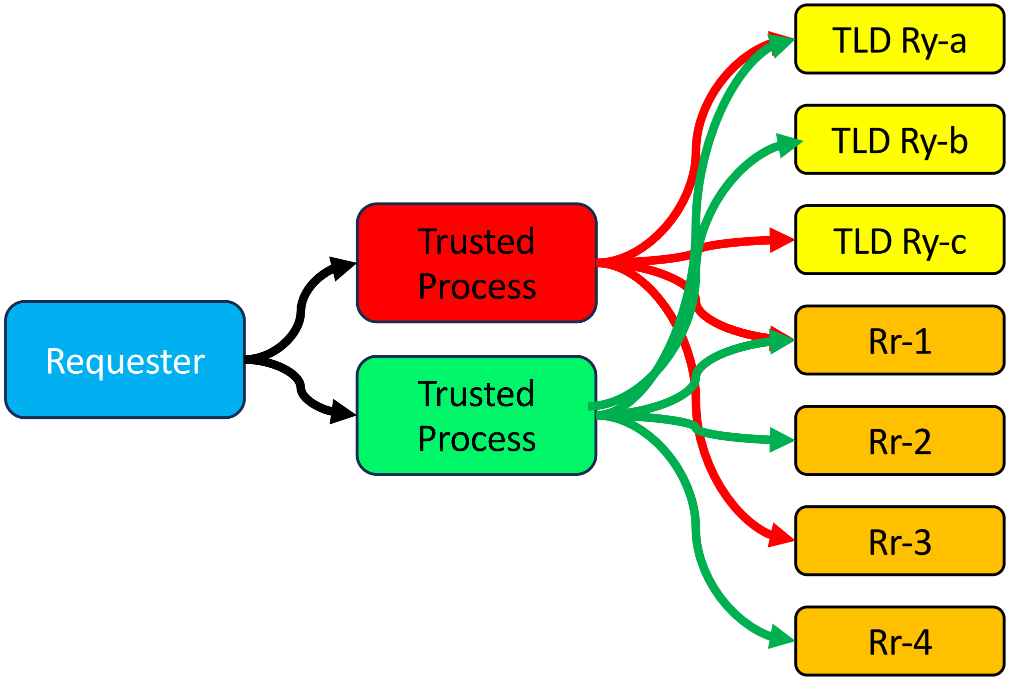


A trusted process can provide the desired functionality.

Limited functionality.

Audited operation.

Trusted Processes



Separate Trusted Processes can provide different services, each with its own set of access control rules, etc.

Policy Specification Tools

Tools

- Collection and Labelling Rulesets
- Illustrative Registrations
- Request Templates
- Request Execution

Collection and Labelling Ruleset

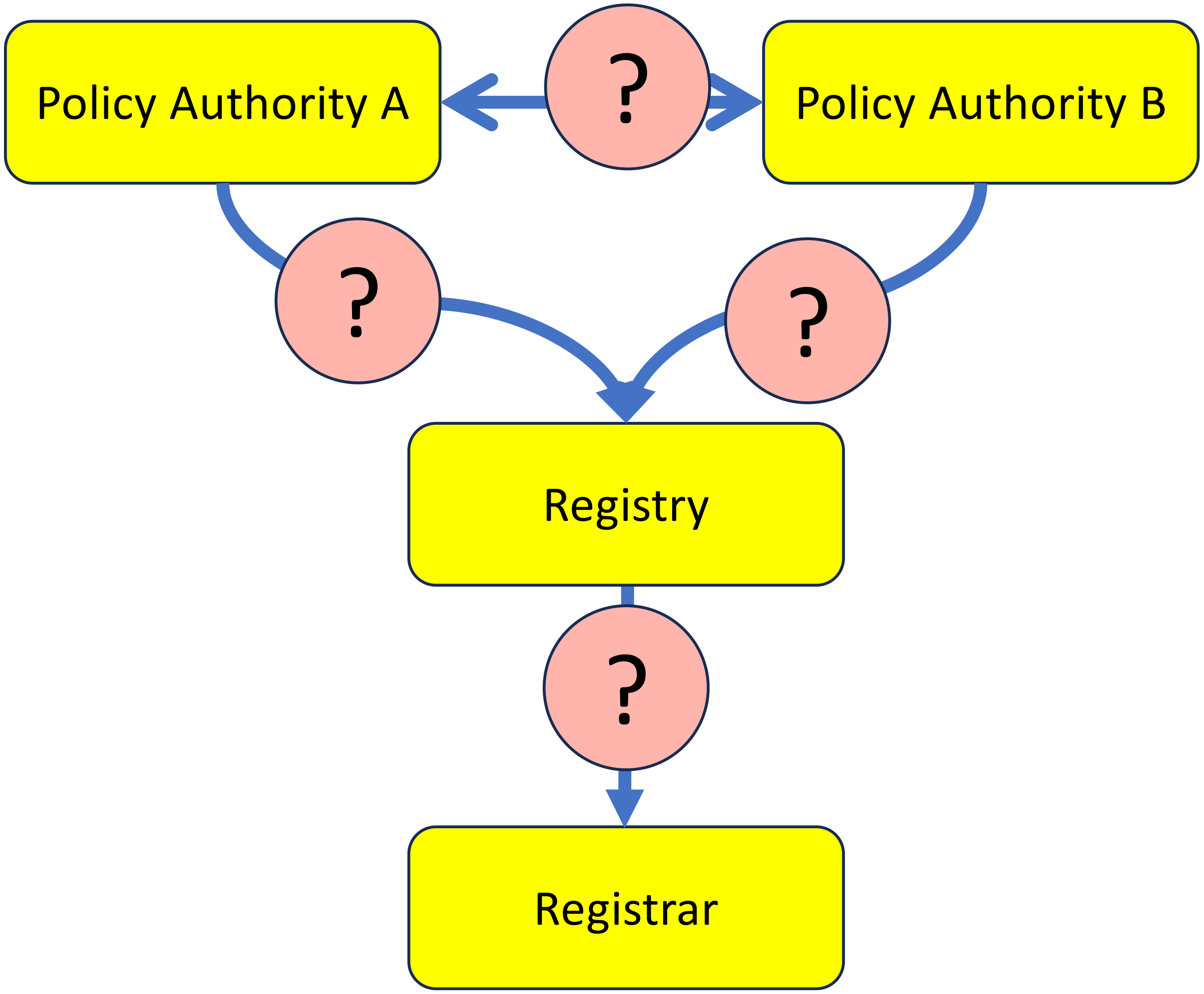
- For each data element
  - Collect/Optional/Don’t Collect
  - Validation Level
  - Sensitivity Level
- Scope – Different rules for different classes of registrants
- Separate ruleset for registrar, registry, policy authority
- Consistency checks

Consistency Checks

- Is the registrar’s policy consistent with the registry’s policy?
- Is the registry’s policy consistent with the policy authority’s policy?

- Are multiple policy authorities consistent with each other?

Consistency Checks



Policy Authority A

?

Policy Authority B

?

?

Registry

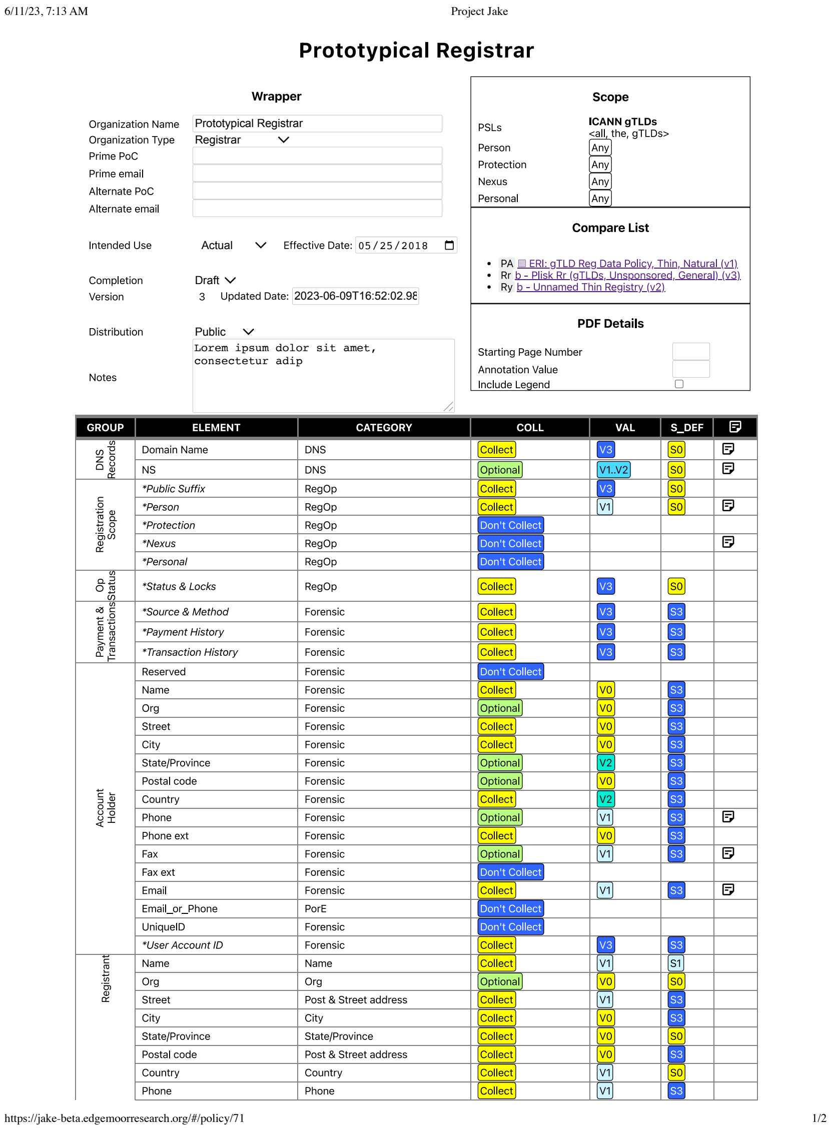
?

Registrar

Request Template

- Template identifier
- Accreditation Authority
- Terms
  - Purpose, obligations
- Allowed Data Elements
- Allowed Sensitivity Levels
- Search permission
- Exigent Circumstances permission
- Log protection permission

Tool Snapshots



6/11/23, 7:13 AM Project Jake

Prototypical Registrar

Wrapper

Organization Name	Prototypical Registrar
Organization Type	Registrar ⌄
Prime PoC	
Prime email	
Alternate PoC	
Alternate email	
Intended Use	Actual ⌄ Effective Date: 05/25/2018
Completion	Draft ⌄
Version	3 Updated Date: 2023-06-09T16:52:02.98
Distribution	Public ⌄
Notes	Lorem ipsum dolor sit amet, consectetur adip

Scope

PSLs	**ICANN gTLDs** <all, the, gTLDs>
Person	Any
Protection	Any
Nexus	Any
Personal	Any

Compare List

- PA ▦ ERI: gTLD Reg Data Policy, Thin, Natural (v1)
- Rr b - Plisk Rr (gTLDs, Unsponsored, General) (v3)
- Ry b - Unnamed Thin Registry (v2)

PDF Details

Starting Page Number	
Annotation Value	
Include Legend	□

GROUP	ELEMENT	CATEGORY	COLL	VAL	S_DEF	🗒
DNS Records	Domain Name	DNS	Collect	V3	S0	🗒
	NS	DNS	Optional	V1..V2	S0	🗒
Registration Scope	*Public Suffix	RegOp	Collect	V3	S0	
	*Person	RegOp	Collect	V1	S0	🗒
	*Protection	RegOp	Don't Collect			
	*Nexus	RegOp	Don't Collect			🗒
	*Personal	RegOp	Don't Collect			
Op Status	*Status & Locks	RegOp	Collect	V3	S0	
Payment & Transactions	*Source & Method	Forensic	Collect	V3	S3	
	*Payment History	Forensic	Collect	V3	S3	
	*Transaction History	Forensic	Collect	V3	S3	
Account Holder	Reserved	Forensic	Don't Collect			
	Name	Forensic	Collect	V0	S3	
	Org	Forensic	Optional	V0	S3	
	Street	Forensic	Collect	V0	S3	
	City	Forensic	Collect	V0	S3	
	State/Province	Forensic	Optional	V2	S3	
	Postal code	Forensic	Optional	V0	S3	
	Country	Forensic	Collect	V2	S3	
	Phone	Forensic	Optional	V1	S3	🗒
	Phone ext	Forensic	Collect	V0	S3	
	Fax	Forensic	Optional	V1	S3	🗒
	Fax ext	Forensic	Don't Collect			
	Email	Forensic	Collect	V1	S3	🗒
	Email_or_Phone	PorE	Don't Collect			
	UniqueID	Forensic	Don't Collect			
	*User Account ID	Forensic	Collect	V3	S3	
Registrant	Name	Name	Collect	V1	S1	
	Org	Org	Optional	V0	S0	
	Street	Post & Street address	Collect	V1	S3	
	City	City	Collect	V0	S3	
	State/Province	State/Province	Collect	V0	S0	
	Postal code	Post & Street address	Collect	V0	S3	
	Country	Country	Collect	V1	S0	
	Phone	Phone	Collect	V1	S3	

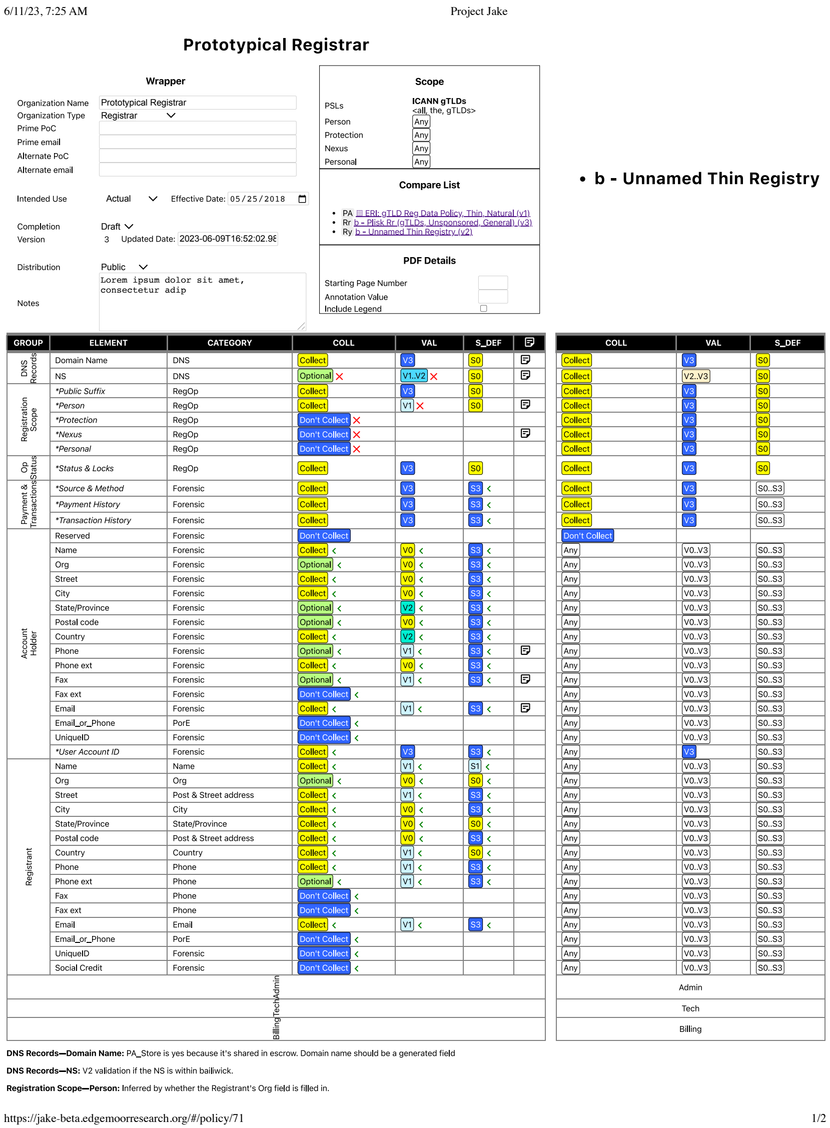
https://jake-beta.edgemoorresearch.org/#/policy/71 1/2

Ruleset for ”Prototypical Registrar”

For each element…

- Coll is Collect, Optional or Don’t Collect
- Val is validation level
  - V0 = accept anything
  - V1 = check syntax
  - V2 = check operational
  - V3 = check identity
- Sens is sensitivity level
  - S0 = public
  - S1 = private
  - S2 = very private
  - S3 = legal paperwork required

Prototypical Registrar Vs Unnamed Thin Registry



6/11/23, 7:25 AM Project Jake

Prototypical Registrar

Wrapper

Organization Name	Prototypical Registrar
Organization Type	Registrar
Prime PoC	
Prime email	
Alternate PoC	
Alternate email	
Intended Use	Actual Effective Date: 05/25/2018
Completion	Draft
Version	3 Updated Date: 2023-06-09T16:52:02.98
Distribution	Public
Notes	Lorem ipsum dolor sit amet, consectetur adip

Scope

PSLs	**ICANN gTLDs** <all, the, gTLDs>
Person	Any
Protection	Any
Nexus	Any
Personal	Any

Compare List

- PA ERI: gTLD Reg Data Policy, Thin, Natural (v1)
- Rr b - Plisk Rr (gTLDs, Unsponsored, General) (v3)
- Ry b - Unnamed Thin Registry (v2)

PDF Details

Starting Page Number

Annotation Value

Include Legend □

GROUP	ELEMENT	CATEGORY	COLL	VAL	S_DEF	🗒	COLL	VAL	S_DEF
DNS Records	Domain Name	DNS	Collect	V3	S0	🗒	Collect	V3	S0
	NS	DNS	Optional ✗	V1..V2 ✗	S0	🗒	Collect	V2..V3	S0
Registration Scope	*Public Suffix*	RegOp	Collect	V3	S0		Collect	V3	S0
	Person	RegOp	Collect	V1 ✗	S0	🗒	Collect	V3	S0
	Protection	RegOp	Don't Collect ✗				Collect	V3	S0
	Nexus	RegOp	Don't Collect ✗			🗒	Collect	V3	S0
	Personal	RegOp	Don't Collect ✗				Collect	V3	S0
Op Status	*Status & Locks*	RegOp	Collect	V3	S0		Collect	V3	S0
Payment & Transactions	*Source & Method*	Forensic	Collect	V3	S3 ‹		Collect	V3	S0..S3
	Payment History	Forensic	Collect	V3	S3 ‹		Collect	V3	S0..S3
	Transaction History	Forensic	Collect	V3	S3 ‹		Collect	V3	S0..S3
Account Holder	Reserved	Forensic	Don't Collect				Don't Collect		
	Name	Forensic	Collect ‹	V0 ‹	S3 ‹		Any	V0..V3	S0..S3
	Org	Forensic	Optional ‹	V0 ‹	S3 ‹		Any	V0..V3	S0..S3
	Street	Forensic	Collect ‹	V0 ‹	S3 ‹		Any	V0..V3	S0..S3
	City	Forensic	Collect ‹	V0 ‹	S3 ‹		Any	V0..V3	S0..S3
	State/Province	Forensic	Optional ‹	V2 ‹	S3 ‹		Any	V0..V3	S0..S3
	Postal code	Forensic	Optional ‹	V0 ‹	S3 ‹		Any	V0..V3	S0..S3
	Country	Forensic	Collect ‹	V2 ‹	S3 ‹		Any	V0..V3	S0..S3
	Phone	Forensic	Optional ‹	V1 ‹	S3 ‹	🗒	Any	V0..V3	S0..S3
	Phone ext	Forensic	Collect ‹	V0 ‹	S3 ‹		Any	V0..V3	S0..S3
	Fax	Forensic	Optional ‹	V1 ‹	S3 ‹	🗒	Any	V0..V3	S0..S3
	Fax ext	Forensic	Don't Collect ‹				Any	V0..V3	S0..S3
	Email	Forensic	Collect ‹	V1 ‹	S3 ‹	🗒	Any	V0..V3	S0..S3
	Email_or_Phone	PorE	Don't Collect ‹				Any	V0..V3	S0..S3
	UniqueID	Forensic	Don't Collect ‹				Any	V0..V3	S0..S3
	User Account ID	Forensic	Collect ‹	V3	S3 ‹		Any	V3	S0..S3
Registrant	Name	Name	Collect ‹	V1 ‹	S1 ‹		Any	V0..V3	S0..S3
	Org	Org	Optional ‹	V0 ‹	S0 ‹		Any	V0..V3	S0..S3
	Street	Post & Street address	Collect ‹	V1 ‹	S3 ‹		Any	V0..V3	S0..S3
	City	City	Collect ‹	V0 ‹	S3 ‹		Any	V0..V3	S0..S3
	State/Province	State/Province	Collect ‹	V0 ‹	S0 ‹		Any	V0..V3	S0..S3
	Postal code	Post & Street address	Collect ‹	V0 ‹	S3 ‹		Any	V0..V3	S0..S3
	Country	Country	Collect ‹	V1 ‹	S0 ‹		Any	V0..V3	S0..S3
	Phone	Phone	Collect ‹	V1 ‹	S3 ‹		Any	V0..V3	S0..S3
	Phone ext	Phone	Optional ‹	V1 ‹	S3 ‹		Any	V0..V3	S0..S3
	Fax	Phone	Don't Collect ‹				Any	V0..V3	S0..S3
	Fax ext	Phone	Don't Collect ‹				Any	V0..V3	S0..S3
	Email	Email	Collect ‹	V1 ‹	S3 ‹		Any	V0..V3	S0..S3
	Email_or_Phone	PorE	Don't Collect ‹				Any	V0..V3	S0..S3
	UniqueID	Forensic	Don't Collect ‹				Any	V0..V3	S0..S3
	Social Credit	Forensic	Don't Collect ‹				Any	V0..V3	S0..S3
Admin							Admin		
Tech							Tech		
Billing							Billing		

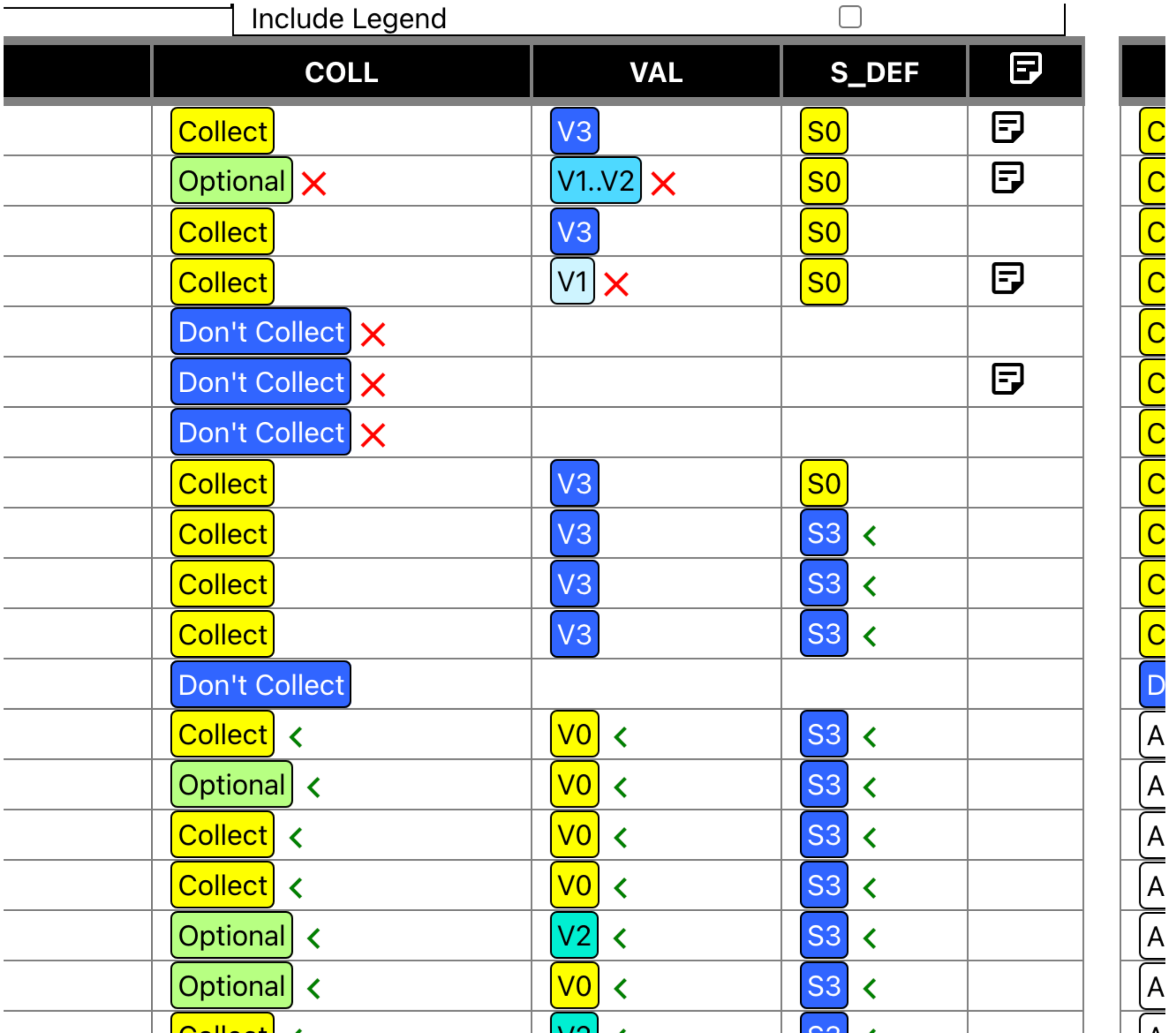
DNS Records—Domain Name: PA_Store is yes because it's shared in escrow. Domain name should be a generated field

DNS Records—NS: V2 validation if the NS is within bailiwick.

Registration Scope—Person: Inferred by whether the Registrant's Org field is filled in.

https://jake-beta.edgemoorresearch.org/#/policy/71 1/2

- **b - Unnamed Thin Registry**



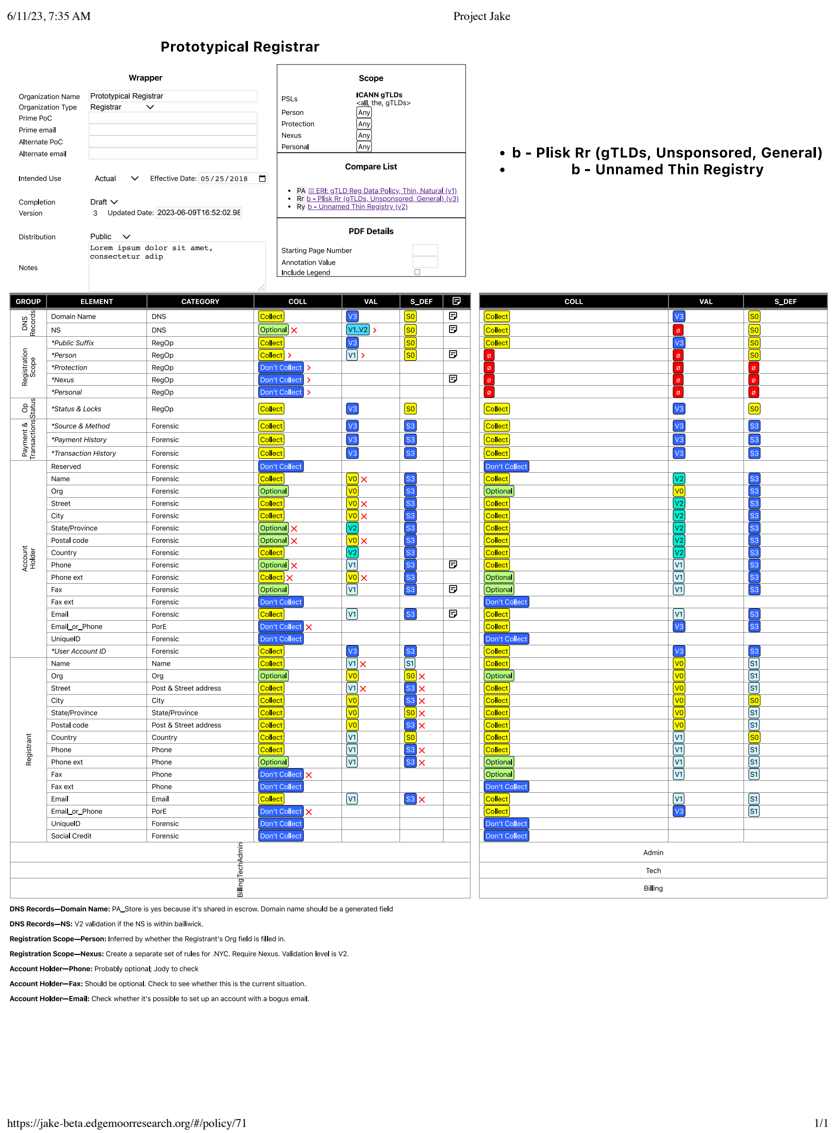
Include Legend ☐

	COLL	VAL	S_DEF	🗒	
	Collect	V3	S0	🗒	C
	Optional ✗	V1..V2 ✗	S0	🗒	C
	Collect	V3	S0		C
	Collect	V1 ✗	S0	🗒	C
	Don't Collect ✗				C
	Don't Collect ✗			🗒	C
	Don't Collect ✗				C
	Collect	V3	S0		C
	Collect	V3	S3 <		C
	Collect	V3	S3 <		C
	Collect	V3	S3 <		C
	Don't Collect				D
	Collect <	V0 <	S3 <		A
	Optional <	V0 <	S3 <		A
	Collect <	V0 <	S3 <		A
	Collect <	V0 <	S3 <		A
	Optional <	V2 <	S3 <		A
	Optional <	V0 <	S3 <		A
	Collect <	V2 <	S3 <		A

X = left ≠ right

< = left is tighter than (consistent) with right

> = left is looser than right



6/11/23, 7:35 AM — Project Jake

Prototypical Registrar

Wrapper

Organization Name: Prototypical Registrar
Organization Type: Registrar
Prime PoC:
Prime email:
Alternate PoC:
Alternate email:

Intended Use: Actual — Effective Date: 05/25/2018

Completion: Draft
Version: 3 — Updated Date: 2023-06-09T16:52:02.98

Distribution: Public

Notes: Lorem ipsum dolor sit amet, consectetur adip

Scope

PSLs: **ICANN gTLDs** <all, the, gTLDs>
Person: Any
Protection: Any
Nexus: Any
Personal: Any

Compare List

- PA ERI: gTLD Reg Data Policy, Thin, Natural (v1)
- Rr b - Plisk Rr (gTLDs, Unsponsored, General) (v3)
- Ry b - Unnamed Thin Registry (v2)

PDF Details

Starting Page Number:
Annotation Value:
Include Legend: □

GROUP	ELEMENT	CATEGORY	COLL	VAL	S_DEF	🗒	COLL	VAL	S_DEF
DNS Records	Domain Name	DNS	Collect	V3	S0	🗒	Collect	V3	S0
	NS	DNS	Optional ✕	V1..V2 ›	S0	🗒	Collect	ø	S0
Registration Scope	*Public Suffix*	RegOp	Collect	V3	S0		Collect	V3	S0
	Person	RegOp	Collect ›	V1 ›	S0	🗒	ø	ø	S0
	Protection	RegOp	Don't Collect ›				ø	ø	ø
	Nexus	RegOp	Don't Collect ›			🗒	ø	ø	ø
	Personal	RegOp	Don't Collect ›				ø	ø	ø
Op Status	*Status & Locks*	RegOp	Collect	V3	S0		Collect	V3	S0
Payment & Transactions	*Source & Method*	Forensic	Collect	V3	S3		Collect	V3	S3
	Payment History	Forensic	Collect	V3	S3		Collect	V3	S3
	Transaction History	Forensic	Collect	V3	S3		Collect	V3	S3
Account Holder	Reserved	Forensic	Don't Collect				Don't Collect		
	Name	Forensic	Collect	V0 ✕	S3		Collect	V2	S3
	Org	Forensic	Optional	V0	S3		Optional	V0	S3
	Street	Forensic	Collect	V0 ✕	S3		Collect	V2	S3
	City	Forensic	Collect	V0 ✕	S3		Collect	V2	S3
	State/Province	Forensic	Optional ✕	V2	S3		Collect	V2	S3
	Postal code	Forensic	Optional ✕	V0 ✕	S3		Collect	V2	S3
	Country	Forensic	Collect	V2	S3		Collect	V2	S3
	Phone	Forensic	Optional ✕	V1	S3	🗒	Collect	V1	S3
	Phone ext	Forensic	Collect ✕	V0 ✕	S3		Optional	V1	S3
	Fax	Forensic	Optional	V1	S3	🗒	Optional	V1	S3
	Fax ext	Forensic	Don't Collect				Don't Collect		
	Email	Forensic	Collect	V1	S3	🗒	Collect	V1	S3
	Email_or_Phone	PorE	Don't Collect ✕				Collect	V3	S3
	UniqueID	Forensic	Don't Collect				Don't Collect		
	User Account ID	Forensic	Collect	V3	S3		Collect	V3	S3
Registrant	Name	Name	Collect	V1 ✕	S1		Collect	V0	S1
	Org	Org	Optional	V0	S0 ✕		Optional	V0	S1
	Street	Post & Street address	Collect	V1 ✕	S3 ✕		Collect	V0	S1
	City	City	Collect	V0	S3 ✕		Collect	V0	S0
	State/Province	State/Province	Collect	V0	S0 ✕		Collect	V0	S1
	Postal code	Post & Street address	Collect	V0	S3 ✕		Collect	V0	S1
	Country	Country	Collect	V1	S0		Collect	V1	S0
	Phone	Phone	Collect	V1	S3 ✕		Collect	V1	S1
	Phone ext	Phone	Optional	V1	S3 ✕		Optional	V1	S1
	Fax	Phone	Don't Collect ✕				Optional	V1	S1
	Fax ext	Phone	Don't Collect				Don't Collect		
	Email	Email	Collect	V1	S3 ✕		Collect	V1	S1
	Email_or_Phone	PorE	Don't Collect ✕				Collect	V3	S1
	UniqueID	Forensic	Don't Collect				Don't Collect		
	Social Credit	Forensic	Don't Collect				Don't Collect		
		BillingTechAdmin					Admin		
							Tech		
							Billing		

DNS Records—Domain Name: PA_Store is yes because it's shared in escrow. Domain name should be a generated field

DNS Records—NS: V2 validation if the NS is within bailiwick.

Registration Scope—Person: Inferred by whether the Registrant's Org field is filled in.

Registration Scope—Nexus: Create a separate set of rules for .NYC. Require Nexus. Validation level is V2.

Account Holder—Phone: Probably optional; Jody to check

Account Holder—Fax: Should be optional. Check to see whether this is the current situation.

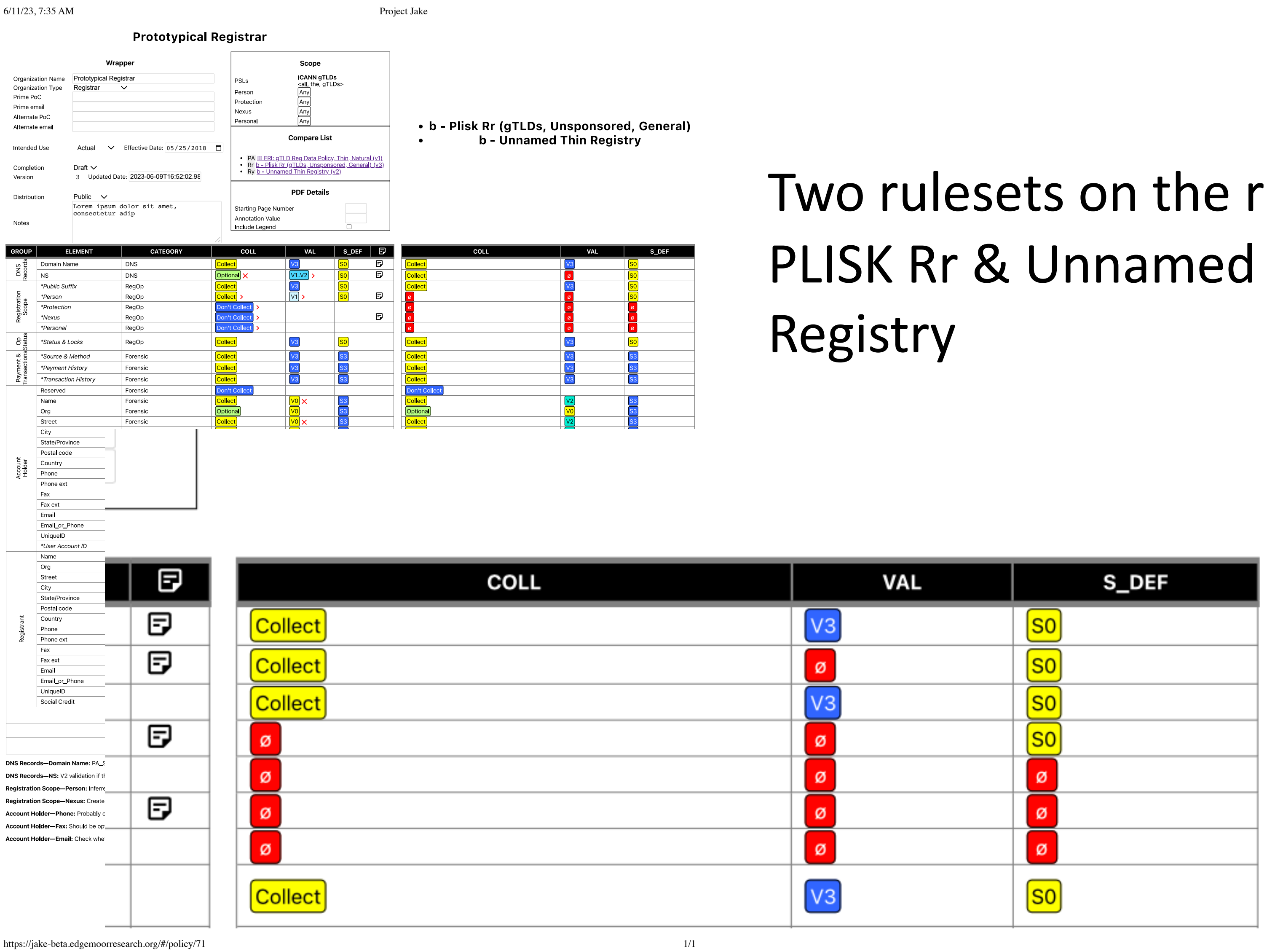
Account Holder—Email: Check whether it's possible to set up an account with a bogus email.

https://jake-beta.edgemoorresearch.org/#/policy/71 — 1/1

- **b - Plisk Rr (gTLDs, Unsponsored, General)**
- **b - Unnamed Thin Registry**

Two rulesets on the right PLISK Rr & Unnamed Thin Registry

Conflicts are in red



6/11/23, 7:35 AM Project Jake

Prototypical Registrar

Wrapper

Organization Name	Prototypical Registrar
Organization Type	Registrar
Prime PoC	
Prime email	
Alternate PoC	
Alternate email	
Intended Use	Actual Effective Date: 05/25/2018
Completion	Draft
Version	3 Updated Date: 2023-06-09T16:52:02.98
Distribution	Public
Notes	Lorem ipsum dolor sit amet, consectetur adip

Scope

PSLs	ICANN gTLDs <all, the, gTLDs>
Person	Any
Protection	Any
Nexus	Any
Personal	Any

Compare List

- PA ERI: gTLD Reg Data Policy, Thin, Natural (v1)
- Rr b - Plisk Rr (gTLDs, Unsponsored, General) (v3)
- Ry b - Unnamed Thin Registry (v2)

PDF Details

Starting Page Number

Annotation Value

Include Legend ☐

GROUP	ELEMENT	CATEGORY	COLL	VAL	S_DEF	🗒	COLL	VAL	S_DEF
DNS Records	Domain Name	DNS	Collect	V3	S0	🗒	Collect	V3	S0
	NS	DNS	Optional ✕	V1..V2 ›	S0	🗒	Collect	ø	S0
Registration Scope	*Public Suffix*	RegOp	Collect	V3	S0		Collect	V3	S0
	Person	RegOp	Collect ›	V1 ›	S0	🗒	ø	ø	S0
	Protection	RegOp	Don't Collect ›				ø	ø	ø
	Nexus	RegOp	Don't Collect ›			🗒	ø	ø	ø
	Personal	RegOp	Don't Collect ›				ø	ø	ø
Op Status	*Status & Locks*	RegOp	Collect	V3	S0		Collect	V3	S0
Payment & Transactions	*Source & Method*	Forensic	Collect	V3	S3		Collect	V3	S3
	Payment History	Forensic	Collect	V3	S3		Collect	V3	S3
	Transaction History	Forensic	Collect	V3	S3		Collect	V3	S3
Account Holder	Reserved	Forensic	Don't Collect				Don't Collect		
	Name	Forensic	Collect	V0 ✕	S3		Collect	V2	S3
	Org	Forensic	Optional	V0	S3		Optional	V0	S3
	Street	Forensic	Collect	V0 ✕	S3		Collect	V2	S3
	City								
	State/Province								
	Postal code								
	Country								
	Phone								
	Phone ext								
	Fax								
	Fax ext								
	Email								
	Email_or_Phone								
	UniqueID								
	User Account ID								
Registrant	Name								
	Org								
	Street								
	City								
	State/Province								
	Postal code								
	Country								
	Phone								
	Phone ext								
	Fax								
	Fax ext								
	Email								
	Email_or_Phone								
	UniqueID								
	Social Credit								

DNS Records—Domain Name: PA_S

DNS Records—NS: V2 validation if t

Registration Scope—Person: Inferre

Registration Scope—Nexus: Create

Account Holder—Phone: Probably c

Account Holder—Fax: Should be op

Account Holder—Email: Check whe

🗒	COLL	VAL	S_DEF
🗒	Collect	V3	S0
🗒	Collect	ø	S0
	Collect	V3	S0
🗒	ø	ø	S0
	ø	ø	ø
🗒	ø	ø	ø
	ø	ø	ø
	Collect	V3	S0

https://jake-beta.edgemoorresearch.org/#/policy/71 1/1

- **b - Plisk Rr (gTLDs, Unsponsored, General)**
- **b - Unnamed Thin Registry**

Two rulesets on the right PLISK Rr & Unnamed Thin Registry