TIER SoR-Registry Core Schema

Early draft of TIER Core Schema for Systems of Record (SoR) and Entity Registry – from Benn Oshrin

There are no required attributes from the perspective of the Core Schema. It is up to a given protocol or implementation to determine what attributes are required, and how such status is conveyed between participants.

Where attributes are multi-valued, it is up to a given protocol or implementation as to whether multiple values are supported, and how such status is conveyed between participants.

Attribute names containing a slash (`/`) may be represented "flat" as listed, or "hierarchical" by removing the slash and establishing a suitable representation in the encoding in use. For example, "name/given" could be represented in JSON as

```
{
  "name":{
    "given":"value"
  }
}
```

Multiple values could be represented as

```
{
  "identifiers":[
    {
      "type":"enterprise",
      "value":"E12345678",
    },
    {
      "type":"network",
      "value":"jqs123"
    }
  ]
}
```

Attribute Release Policy

Attribute Release Policies are encoded in metadata, as described below. The following policies are defined:

- `public`: The attribute and value may be used without restriction.
- `internal`: The attribute and value are to be used for official institutional purposes only, and may not be redistributed without permission.
- `private`: The attribute and value may not be used for any purpose without permission.

Attribute Data Types

- binary
- boolean
- country: ISO 3166-1 two letter country code
- date: YYYY-MM-DD format (ISO 8601)
- dateTerm: A datestamp used to indicate intervals such as a semester, trimester, or quarter. The general format is YYYY-L#, where L is one of H (half year), T (third), or Q (quarter), and # is the sequential number. eg: 2015-H2 designates the second semester of the 2015 academic year (and so might physically be in the year 2016).
- dateTime: YYYY-MM-DDTHH:MM:SSZ format (ISO 8601)
- integer
- locale: LL_CC format (ISO 639-1 two letter language code, an underscore, ISO 3166-1 two letter country code)
- region: ISO 3166-2 subdivision code, not including country prefix (eg: `BC` not `CA-BC`)
- string: Strings are case-preserving but not case-sensitive
- extensibleVocabulary: The Core Schema vocabulary should be supported when described values are relevant, however implementations may add to the vocabulary. How supported values are conveyed between participants is outside of the scope of this document. Extended vocabulary must begin with `x-`.

Case Sensitivity

All attribute names and other elements specified here are case sensitive. eg: `official` and `OFFICIAL` are *not* the same.

Metadata

Any complex attribute (Person, Person Role, Address, Identifier, etc) may optionally have the following meta attributes:

- `meta/created`: Timestamp of record creation, in dateTime format
- `meta/id`: Identifier for this specific (sub)attribute
- `meta/lastModified`: Timestamp of last modification, in dateTime format
- `meta/release`: Attribute release policy, as described above

Person Core Attributes

Attribute	Data Type	Definition	Multi-Valued? (Parent Attribute)
`address`			Yes (`addresses`)
`address/country`	country	Country from a postal address	One per parent object
`address/formatted`	string	Address rendered as a single string, possibly with embedded newlines (`\n`)	One per parent object
`address/locality`	string	Locality information from a postal address (city, etc)	One per parent object
`address/language`	locale	The language encoding of the address	One per parent object
`address/postalCode`	string	Postal code from a postal address	One per parent object
`address/region`	region	Region information from a postal address (state, province, etc)	One per parent object
`address/room`	string	Room information from a postal address	One per parent object
`address/street` ⚠ Changing to `streetAddress`	string (multi-line)	Street/site information from a postal address (street name, house number, etc)	One per parent object
`address/type`	extensibleVocabulary: • `campus` • `home` • `office` • `parent` • `postal` • `summer` • `former-`*anytype*	The type of the address	One per parent object
`address/verified`	boolean	True if the address has been verified	One per parent object
`citizenship`	country	Country of citizenship of the person	Yes (`citizenships`)
`dateOfBirth`	date	The date of birth of the person	No
`emailAddress`			Yes (`emailAddresses`)
`emailAddress/address`	string	The email address	One per parent object
`emailAddress/type`	extensibleVocabulary: • `delivery` • `department` • `department-`*deptlabel* • `forwarding` • `official` • `personal` • `preferred` • `former-`*anytype*	The type of the email address	One per parent object
`emailAddress /verified`	boolean	True if the address has been verified	One per parent object
`ethnicity`	extensibleVocabulary: • `africanAmerican` • `alaskaNative` • `americanIndian` • `asian` • `hispanic` • `nativeHawaiian` • `other` • `pacificIslander` • `white`	The ethnicity of the person ([US Census](#))	Yes (`ethnicities`)

gender	extensibleVocabulary: • `female` • `male`	The gender of the person	No
`identifier`			Yes (`identifiers`)
`identifier` `/identifier`	string	The identifier	One per parent object

`identifier/type`	extensibleVocabulary:
	
	• `badge`
	• `badge-`
	  `barcode`
	• `badge-chip`
	• `badge-`
	  `magstripe`
	• `enterprise`
	• `national`
	• `network`
	• `referenceId`
	• `role`
	• `role-`
	  `affiliate`
	• `role-alumni`
	• `role-`
	  `employee`
	• `role-guest`
	• `role-student`
	• `sor`
	• `sor-`
	  `affiliate`
	• `sor-alumni`
	• `sor-employee`
	• `sor-guest`
	• `sor-student`
	• `former-`*anyty*
	  pe
		The type of the identifier
		
		• badge: Identifier as encoded on a badge/physical ID card
		• badge-barcode: Identifier as encoded on a 1D or 2D barcode printed on a badge
		• badge-chip: Identifier as stored on a smart chip (contact or NFC) embedded in a badge
		• badge-magstripe: Identifier as encoded on a magnetic stripe of a badge
		• enterprise: Persistent identifier used to uniquely identify an individual across the enterprise
		• national: Government issued identifier (eg: SSN)
		• network: Identifier used for access to network services (eg: NetID)
		• referenceId: An ID Match reference identifier
		• role: Persistent identifier for a given role, used by an individual system of record and/or registry
		• role-*: Persistent identifier for a given role assigned by the specified system of record
		• sor: Persistent identifier used by an individual system of record
		• sor-*: Persistent identifier assigned by the specified system of record
			One per parent object

`identityProof`			Yes (`identityProofs`)
`identityProof` `/dateOfBirth`	date	Date of birth, as confirmed on document	One per parent object
`identityProof` `/documentIssuer`	string	Name of agency issuing the confirmation document	One per parent object
`identityProof` `/documentType`	extensibleVocabulary: • `driversLicen` `se` • `national` • `passport` • `regional` • `tribal`	Type of document used to confirm identity • driversLicense: Photo ID used to license drivers • national: ID issued by a national government, other than drivers licenses or passports • passport: Passport, including Passport Cards • regional: ID issued by a regional government (such as states or provinces), other than drivers licenses • tribal: ID issued by a tribal government (such as Native American tribes)	One per parent object
`identityProof` `/fullName`	string	Full name, as confirmed on document	One per parent object
`identityProof/status`	extensibleVocabulary: • `expired` • `invalid` • `valid`	Status of the identity proofing	One per parent object
`identityProof` `/timeVerified`	dateTime	Time document was confirmed	One per parent object
`identityProof` `/verifiedAddress`	string	Address, as confirmed on document	One per parent object
`name`			Yes (`names`)
`name/family`	string	The component of the person's name excluding the given, middle, and honorific components	One per parent object
`name/formatted`	string	The person's name, suitably formatted for display	One per parent object
`name/given`	string	The component of the person's name excluding the middle, family, and honorific components	One per parent object
`name/language`	locale	The language encoding of the person's name	One per parent object

name/middle	string	The component of the person's name excluding the given, family, and honorific components	One per parent object
name/prefix	string	The honorific prefix of the person's name, such as "Dr" or "Ms"	One per parent object
name/suffix	string	The honorific suffix of the person's name, such as "Jr" or "III"	One per parent object
name/type	extensibleVocabulary: `author` `fka` `official` `preferred`	The type of the name - author: Name suitable for publishing (eg: on academic papers) - fka: "Formerly Known As", a previous name for the person (eg: maiden name) - official: Name as found on government-issued ID - preferred: Name as self-asserted	One per parent object
photo			Yes (`photos`)
photo/data	binary	Encoding of a photo of the person	One per parent object
photo/encoding	extensibleVocabulary: `bmp` `gif` `jpg` `png` `tiff`	The encoding used for the photo	One per parent object
photo/type	extensibleVocabulary: `badge` `official` `personal`	The type of the photo (*not* the encoding) - badge: Photo used on an ID card - official: Photo taken for official purposes (such as display in a faculty directory) - personal: User supplied photo for non-official purposes	One per parent object
primaryAffiliation	string	The primary affiliation for the person, as defined by the institution (values same as for Person Role *affiliation* attribute, below)	No
primaryCampus	string	The primary campus location for the person, as defined by the institution	No
role		Parent attribute for Role attributes, described below	Yes
telephoneNumber			Yes (`telephoneNumbers`)
telephoneNumber /number	string	Telephone number for the person, preferably in + notation	One per parent object
telephoneNumber/type	extensibleVocabulary: `campus` `fax` `home` `mobile` `office` `summer` `former-`*anytype*	The type of the telephone number	One per parent object
telephoneNumber /verified	boolean	True if the telephone number has been verified	One per parent object
test	boolean	True if this record represents a test entry	No
url			Yes (`urls`)
url/url	string	URL for the person	One per parent object
url/type	extensibleVocabulary: `official` `personal`	The type of the telephone number	One per parent object

| visa | extensibleVocabulary:

• `permanentRes ident`
• `A`
• `A-2`
• `B-1`
• `B-2`
• `BCC`
• `C`
• `CR1`
• `D`
• `E`
• `E-3`
• `F`
• `G-1`
• `G-2`
• `G-3`
• `G-4`
• `G-5`
• `H-1B`
• `H-1B1`
• `H-2A`
• `H-2B`
• `H-3`
• `I`
• `IR1`
• `J`
• `K-1`
• `K-3`
• `L`
• `M`
• `NATO`
• `P`
• `Q`
• `T`
• `TD`
• `TN`
• `U` | Visa status of the person | No |

Person Role Core Attributes

Attribute	Data Type	Definition	Multi-Valued?
`address`		*As defined for Person Attributes*	Yes (`addresses`)
`affiliation`	extensibleVocabulary: • `affiliate` • `alum` • `employee` • `faculty` • `library-walk-in` • `member` • `staff` • `student`	The person's broad relationship to the institution for the role ([eduPerson](#))	One per role
`campus`	string	The campus location this role is attached to, as defined by the institution	Yes (`campuses`)
`campusCode`	string	Machine readable identifier for a campus. This value is unlikely to have meaning outside of a specific institution.	Yes (`campusCodes`)
`department`	string	The name of the department the role is attached to (multiple values are permitted if multiple departments sponsor a single role)	Yes (`departments`)
`departmentCode`	string	Machine readable identifier for a department. This value is unlikely to have meaning outside of a specific institution.	Yes (`departmentCodes`)
`displayTitle`	string	The display title for this role	One per role
`emailAddress`		*As defined for Person Attributes*	Yes (`emailAddresses`)
`identifier`		*As defined for Person Attributes*	Yes (`identifiers`)
`leaveBegins`	dateTime	Time at which leave from this role begins; advisory – `status` is controlling	One per role
`leaveEnds`	dateTime	Time after which leave from this role is no longer in effect; advisory – `status` is controlling	One per role
`manager`	string	An identifier (preferably of type `enterprise`) describing the manager for this role ⚠️ This should become a complex attribute (identifier+type)	Yes (`managers`)

organization	string	The name of the organization/institution the role is attached to (multiple values are permitted if multiple organizations sponsor a single role)	Yes (`organizations`)
organization Code	string	Machine readable identifier for an organization. This value is unlikely to have meaning outside of a specific institution.	Yes (`organization Codes`)
percentTime	integer (0 - 100)	The percentage time for this role (100 = full time)	One per role
rank	positive integer	The rank of this role relative to *all* roles from all SORs (highest rank = 1)	One per role
rankSor	positive integer	The rank of this role relative to_ only_ roles from this SOR (highest rank = 1)	One per role
roleBegins	dateTime	Time at which the role officially begins	One per role
roleEnds	dateTime	Time after which the role is officially no longer in effect	One per role
sor	string	Label for the system of record asserting this role	One per role
sponsor	string	An identifier (preferably of type `enterprise`) describing the sponsor for this role ⚠️ This should become a complex attribute (identifier+type)	Yes (`sponsors`)
status	extensibleVocabulary: `accepted` `applied` `active` `offered` `onLeave` `registered` `suspended` `terminated`	Status associated with this role: - The person has accepted an offer for this role (enrollment or hire) - The person has applied for this role (enrollment or hire) - The role is active (hire) - The person has been made an offer for this role but has not yet accepted (enrollment or hire) - The person is on leave from this role (enrollment or hire) - The person has registered for this role (enrollment) - The person has been suspended from this role (enrollment or hire) - The role has been terminated (enrollment or hire) (termination date is in `roleEnds`)	One per role
telephoneNumber		*As defined for Person Attributes*	Yes (`telephoneNumbers`)
terminationReason	extensibleVocabulary: `deceased` `graduated` `involuntary` `resigned` `retired` `withdrew`	Reason for termination associated with this role	One per role
title	string	The official title for this role	Yes (`titles`)
url		*As defined for Person Attributes*	Yes (`urls`)
validFrom	dateTime	Time at which services associated with the role should begin	One per role
validThrough	dateTime	Time after which services associated with the role should be terminated	One per role

HR Person Role Attributes

Attribute	Data Type	Definition	Multi-Valued?
employeeType	extensibleVocabulary: `consultant` `contractor` `emeritus` `exempt` `regular` `tenured` `vendor` `visiting` `workStudy`		No

Student Person Role Attributes

Attribute	Data Type	Definition	Multi-Valued?

classYear	extensibleVocabulary: • freshman • sophomore • junior • senior • ####	#### is a four digit expected year of graduation	No
courseAffiliation	extensibleVocabulary: • Administrator • ContentDeveloper • Instructor • Learner • Manager • Member • Mentor • Officer • TeachingAssistant	Person's affiliation/role with a course. Based on MACE-Dir work.	Yes, per-courseMembership
courseMembership	string		Yes
degree	extensibleVocabulary: • AAS • BA • BFA • BS • DDS • DNP • JD • LLM • MA • MArch • MBA • MD • MFA • MPH • MPS • MS • PhD		Yes, if a single program generates more than one degree. (Otherwise use separate roles.)
major			Yes (majors)
major/major	string	Student's major	No
major/majorCode	string	Machine readable identifier for the major. This value is unlikely to have meaning outside of a specific institution.	No
major/type	extensibleVocabulary • dual • minor • primary • secondary		No
residenceHall	string		No
studentType	extensibleVocabulary: • continuing • graduate • nondegree • professional • secondary • summer • undergraduate • visiting	Secondary = (eg) high school	No
term	dateTerm	Term for which this record applies	No

College/School should be expressed in `organization` and Major/Program should be expressed in `department`. (XXX or should they get dedicated attributes?)

Extended Attributes

The Core Schema may be extended. How extended attributes are conveyed between participants is outside of the scope of this document. Extended attributes must begin with `x-`, may be hierarchical, and may be attached to the Person or Person Role.

ⓘ **Comments from Eric Goodman, Responses from Chris Hyzer**

Challenging to comment on (especially on a fairly quick read!) So this is kind of a dartboard throw of questions and comments as I read through.

- General note: this construction would seem to put a fairly strict set of requirements on the actual registry repository. Yes, it's possible to convert, but these structures and hierarchies are pretty specific in ways that would be more complex to abstract; it's not just renaming values.
- Most of the attributes I'm looking at are defined with "ExtensibleVocabulary". Is the idea that the "base" vocabulary is fixed (but extendable), or that the default vocabulary be ignored? I'm also concerned about the requirement for the "x-" prefix on any extensions, but I understand the argument for it.
    - ChrisH: I think that needs to be updated based on the TIER common elements document. Maybe just linked to it, no need to mention in each API
- For example, most campuses I'm aware of would call an ID a "Student ID", not an "sor-studentsystem" ID. (Even though in many cases the latter might be a more accurate value.) Perhaps that could be handled with a simple rewrite rule on a ESB; I'd need to think about it more.
- On the Attribute Release Policies, is there any metadata associated with them? There are many attributes that will have "well understood" (well, supposedly well understood) campus release/usage policies associated with them. Does this model provide a mechanism to expand them if necessary?
- Is the idea that SSN is encoded as "identifier/type=national" (and presumedly "ARP=private")? Would take getting my head around that approach, where each ID has its own ARP but they are all grouped together as a single list. Should consider a mechanism for vaulting these. Hashing is generally not useful (security wise, though maybe it is compliance wise), encrypting impacts your ability to do matching. Not sure what to do here, but I don't think just having SSN sitting there is a good idea.
- Mentioned elsewhere, I don't like that the only conditions on roles are start and end dates. But it seems like "roles" in this context are really "affiliations", and other roles of the authZ type would perhaps be outsourced to, e.g., Grouper? In any case, if affiliation is what's meant, the limitation is less concerning (and also, additional conditions could be added in the future).
- Not clear on the intent of "manager". Is it equivalent to "supervisor"?

ⓘ **Comments from Tom Jordan**

On the TIER SoR-Registry Core Schema:

1. Provided there is a mechanism for extending attributes, I believe that base attributes and extended attributes can coexist. I would envision that Wisconsin would both supplement the existing role types and create new ones, but for the most part I believe that we can successfully map to the existing core attributes. I do envision a number of other types of roles that could be represented and possible attribute name conflicts (for example 'department' relating to both employment, affiliate, emeritus, etc) so unless the role is encapsulated in a data structure that disambiguates, they may need to be prefixed or named differently.
2. Unless I'm misunderstanding the model, some of the person role core attributes tied to the person object are perhaps more appropriate to roles. For us at least, attributes like manager, organization, and department are going to be specific to a person's job, and of course they may have more than one. Likewise for campus codes when we roll up into our systemwide identity registry.
3. I think the registry model needs to be able to provide non-normalized storage of role information as well (for example, student information as expressed in the SIS vernacular) so that connected systems at least have the capability to retrieve and consume source-specific terms that may need to correlate to terms in other campus systems. This could perhaps be achieved through extended attributes in the current structure, but may require more complex data structures that would suggest that having the ability to declare a different role type (or a branch beneath an existing role type) might be better.
4. I like the idea of metadata regarding attribute release on a per-complex-attribute basis. Would it be possible to extend this model to all attributes? Some of the attributes that are most likely to require privacy controls (address, email, etc) are not listed as complex.

Tom