

Towards Viable Information Infrastructures for Trustworthy Networking

Random, General Thoughts
Illustrated with Frustrations from Robust Interdomain Routing

Doug Montgomery (dougm@nist.gov)

<https://www.nist.gov/programs-projects/robust-inter-domain-routing>

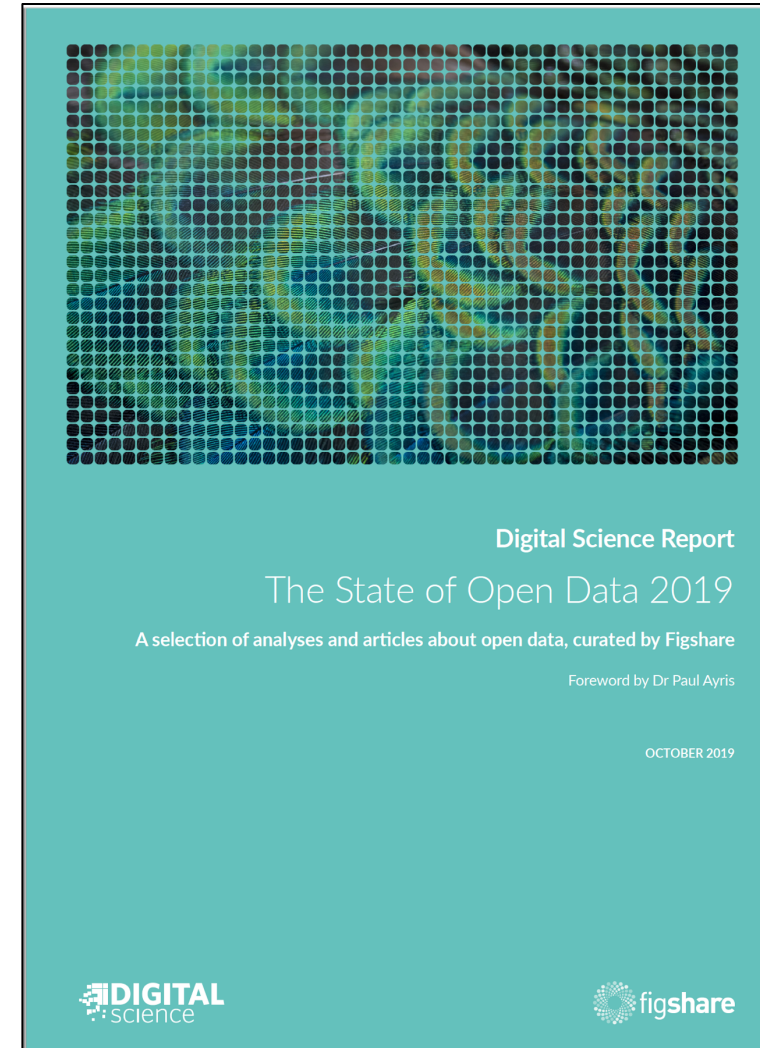
Open Knowledge Network ?

• OKN-KISMET

- Outline research agenda.
- The goal is to start thinking about ...something with "transformative impact".

• What are others thinking?

- The State of Open Data 2019
 - https://digitalscience.figshare.com/articles/The_State_of_Open_Data_Report_2019/9980783
- FAIR - Findable, Accessible, Interoperable, Reusable
 - <https://www.go-fair.org/fair-principles/>
- Internet of FAIR Data & Services
 - <https://www.go-fair.org/resources/internet-fair-data-services/>
- Creating Value From Open Data
 - https://www.europeandataportal.eu/sites/default/files/edp_creating_value_through_open_data_0.pdf
- Open Government Data Act
 - <https://www.data.gov/open-gov/>



GO FAIR - Findable, Accessible, Interoperable, Reusable

<https://www.go-fair.org/fair-principles/>

- **Findable**

The first step in (re)using data is to find them. Metadata and data should be easy to find for both humans and computers. Machine-readable metadata are essential for automatic discovery of datasets and services.

- (Meta)data are assigned a globally unique and persistent identifier
- Data are described with rich metadata
- Metadata clearly and explicitly include the identifier of the data they describe
- (Meta)data are registered or indexed in a searchable resource

- **Accessible**

Once the user finds the required data, she/he needs to know how can they be accessed, possibly including authentication and authorization.

- (Meta)data are retrievable by their identifier using a standardised communications protocol
- The protocol is open, free, and universally implementable
- The protocol allows for an authentication and authorisation procedure, where necessary
- Metadata are accessible, even when the data are no longer available

- **Interoperable**

The data usually need to be integrated with other data. In addition, the data need to interoperate with applications or workflows for analysis, storage, and processing.

- (Meta)data use a formal, accessible, shared, and broadly applicable language for knowledge representation.
- (Meta)data use vocabularies that follow FAIR principles
- (Meta)data include qualified references to other (meta)data

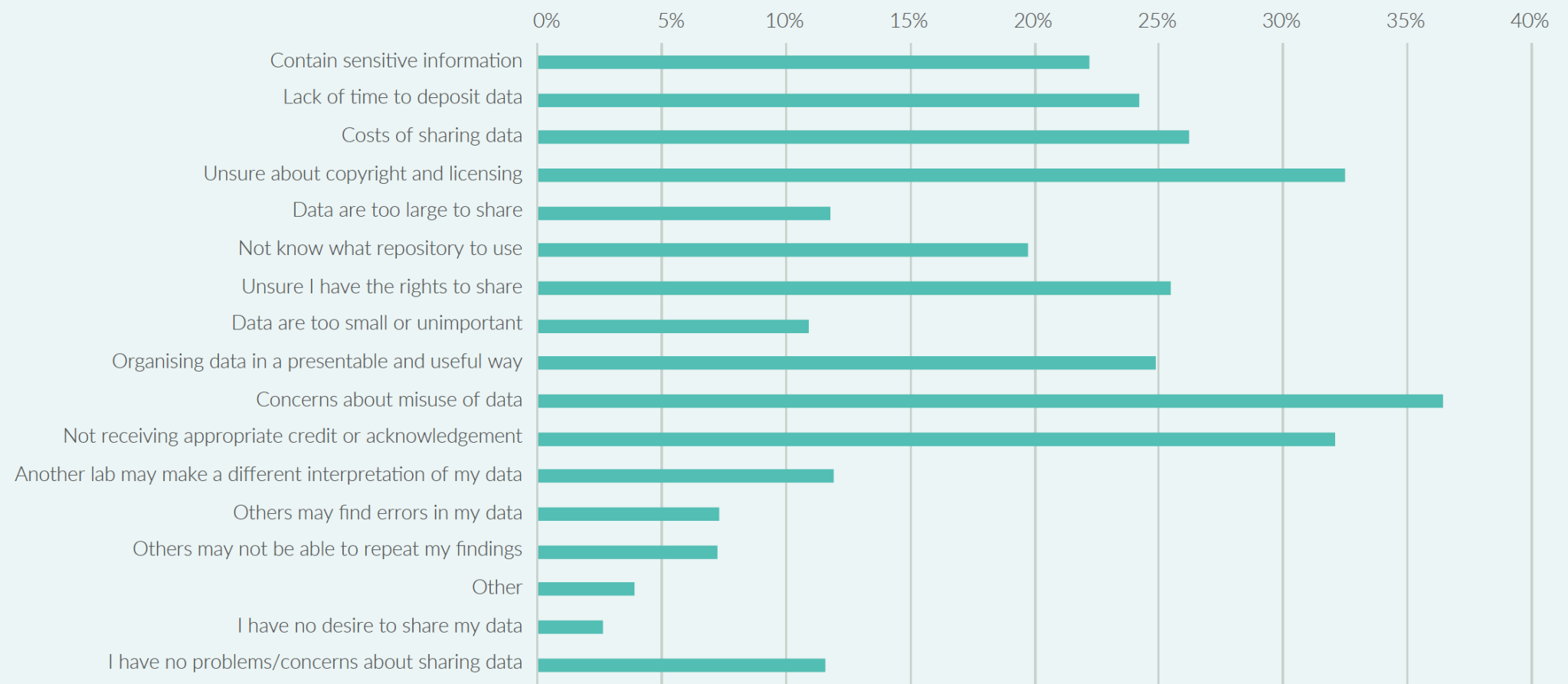
- **Reusable**

The ultimate goal is to optimize the reuse of data. To achieve this, metadata and data should be well-described so that they can be replicated and/or combined in different settings.

- Meta(data) are richly described with a plurality of accurate and relevant attributes
- (Meta)data are released with a clear and accessible data usage license
- (Meta)data are associated with detailed provenance
- (Meta)data meet domain-relevant community standards

Barriers to Open Knowledge Networks?

Problems/concerns respondents have with sharing datasets



https://digitalscience.figshare.com/articles/The_State_of_Open_Data_Report_2019/9980783

BGP “Robustness Data” and OKNs?

Info Infrastructure for Trustworthy BGP

• Producers

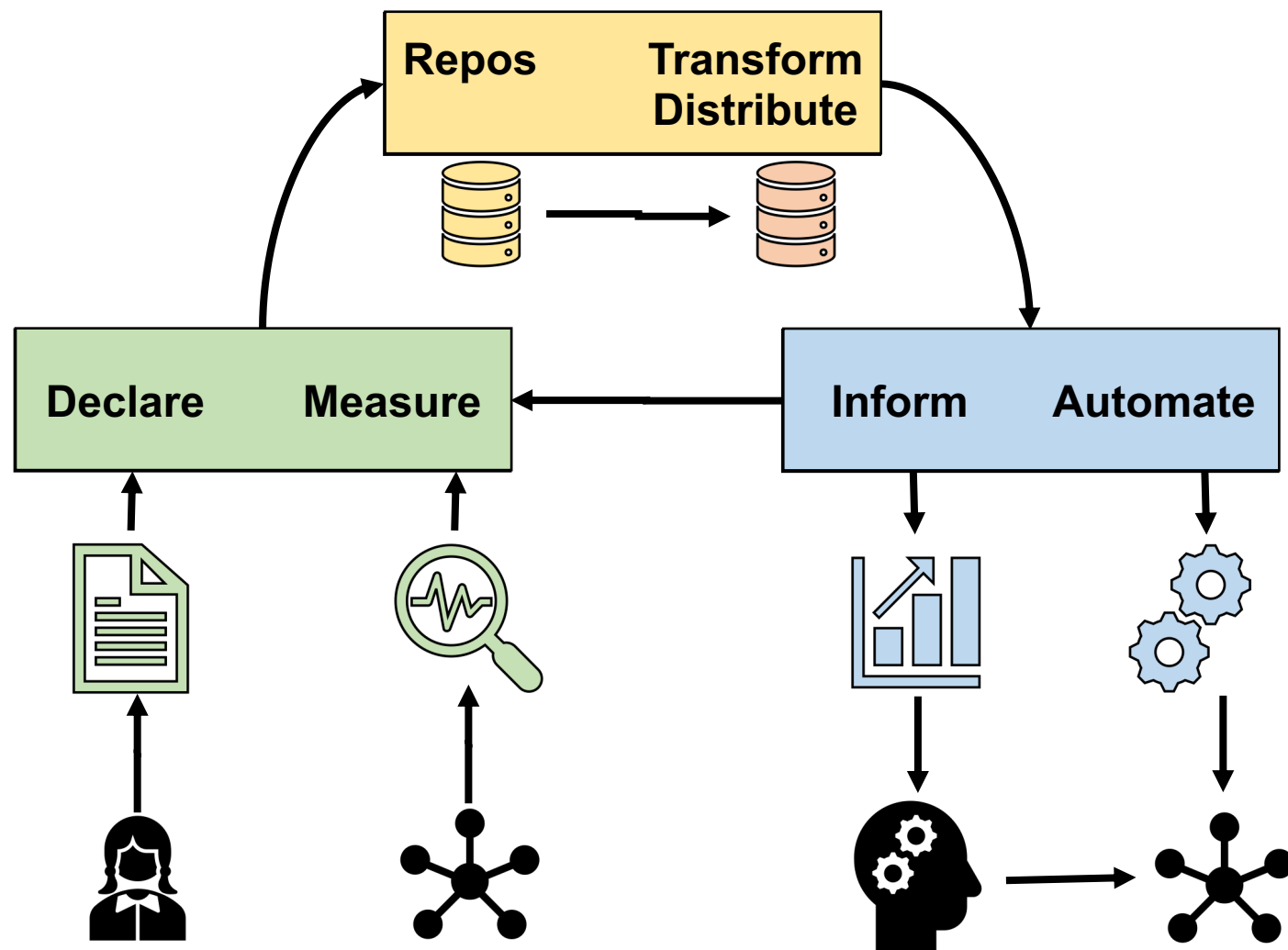
- Declarative
 - Whois, RPKI, IRR
- Measured
 - Routeviews, RIS

• Data

- Repositories
 - RPKI, Routeviews
- Intermediaries

• Consumers

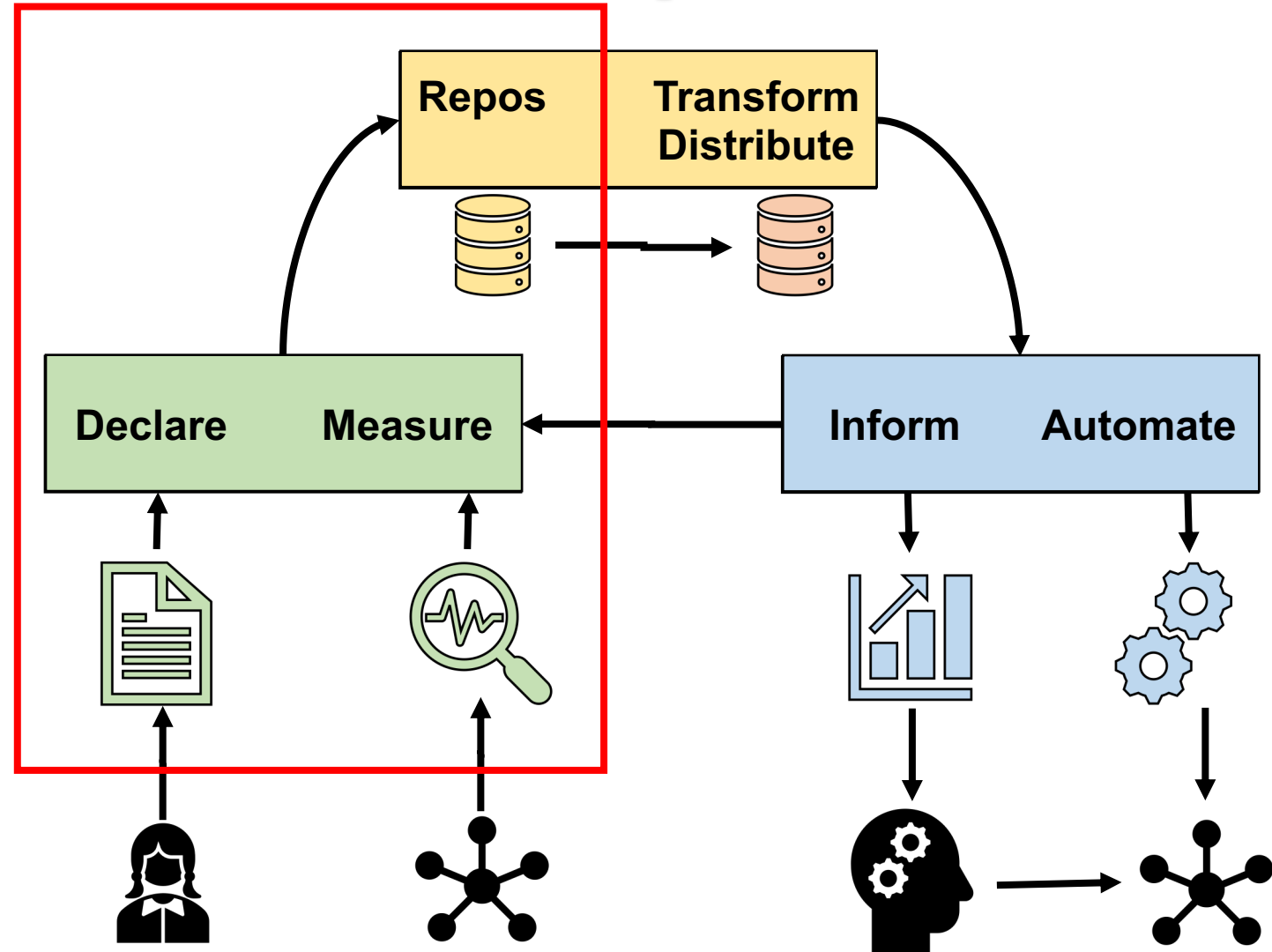
- Informative
 - Publications, Anomaly Detectors
- Automation
 - BGP Route Filters, SAV



Information Infrastructure Properties

• Producers

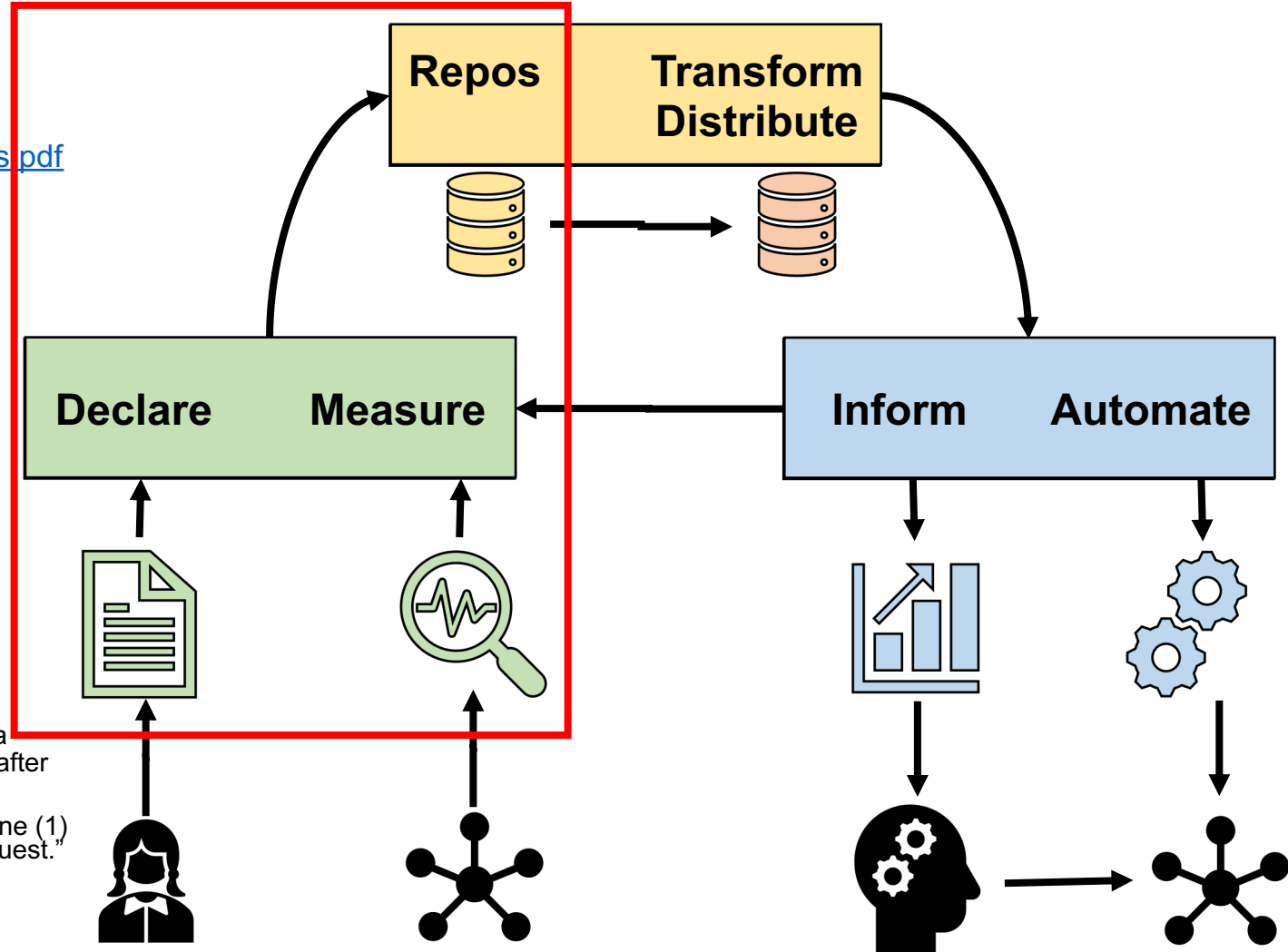
- Access control & Authentication
 - Who / what provides input
 - How do you verify above?
- Information Quality
 - Correctness
 - Completeness
 - Uncertainty
- Responsiveness / Liveness
 - Input stimulus to repository
 - Purging stale data



Information Infrastructure Properties

• BGP Producers

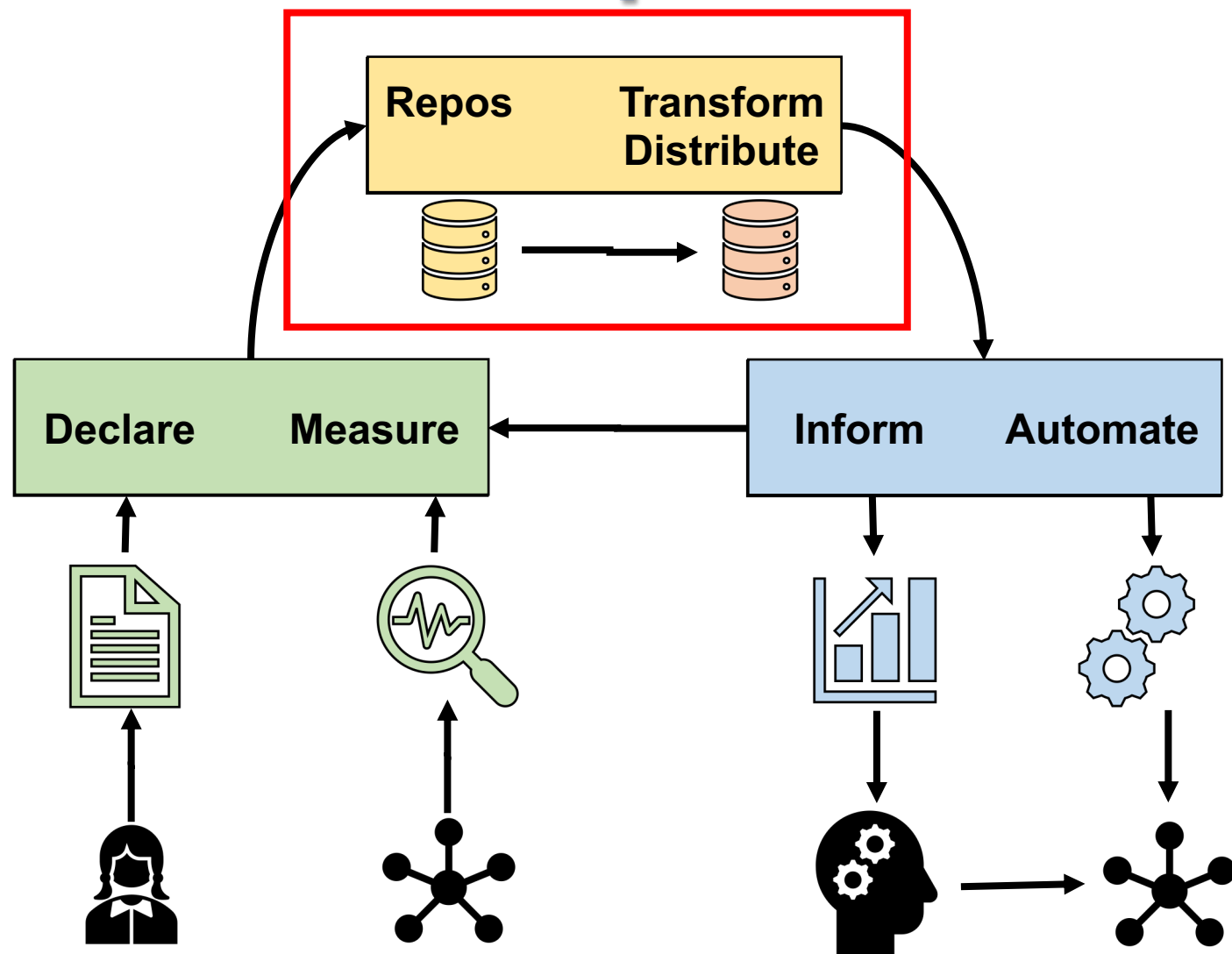
- CPS – Certificate Practice Statement
 - <https://www.arin.net/resources/manage/rpki/cps.pdf>
- RPKI
 - Strong Access control & Authentication Model
 - ARIN – constrained by implications of RSA.
- Information Quality
 - Mechanisms to help users avoid input errors.
 - Informal efforts to scrub RPKI data with measurement data.
- Measurement data is ground truth?
 - How do we know that BGP data sent to collector is not malicious?
- Responsiveness / Liveness
 - CPS – a vague SLA?
 - Designed for resource assignment & transfer.
 - “ARIN expects to issue a certificate attesting to a resource allocation within one (1) business day after approval of the allocation.”
 - “ARIN will process a revocation request within one (1) business day of receipt and validation of the request.”
 - Need data on measured performance of RPKI production system.



Information Infrastructure Properties

• Data Repositories

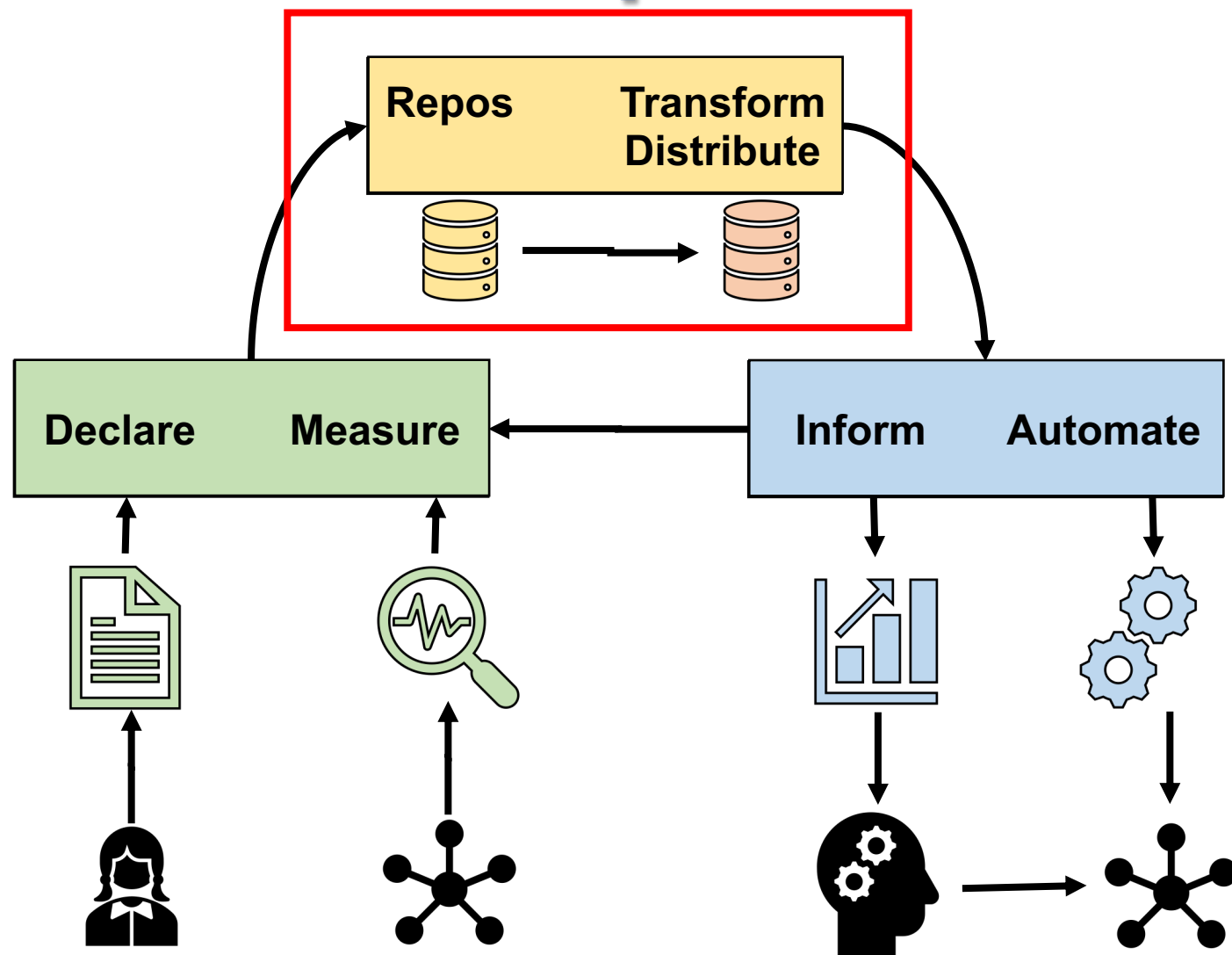
- Access control & Authentication
 - Who / what can access data?
 - How do you verify above?
 - Privacy issues?
- Information Quality
 - Meta data for completeness, correctness, uncertainty?
- Repository Quality
 - Integrity / Availability
- Transformation / Distribution
 - To promote interoperability
 - To foster adoption / use
 - To scale dissemination



Information Infrastructure Properties

• BGP Data Repositories

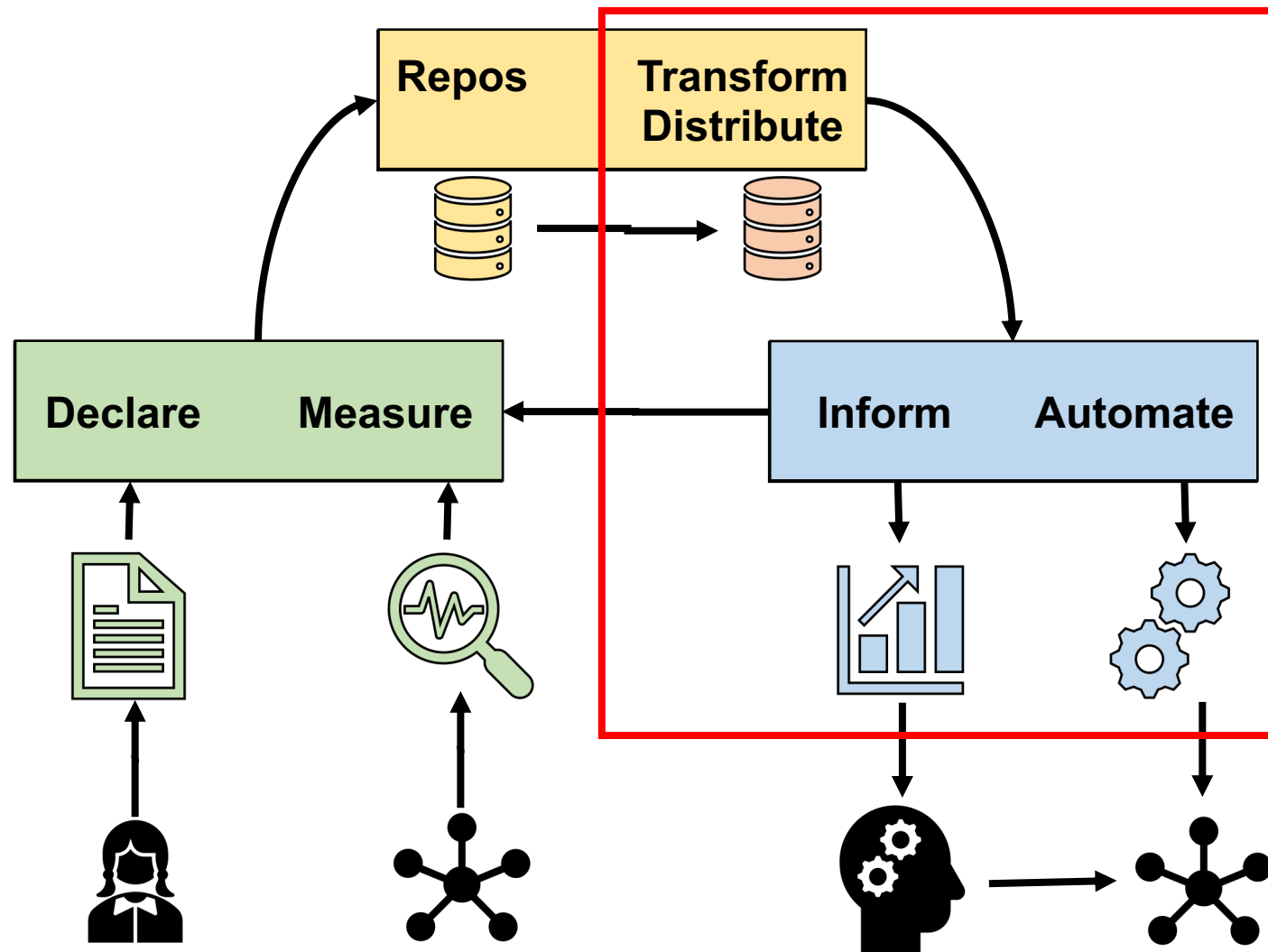
- RPKI
 - ARIN - Must accept Relying Party Agreement (RPA) to access data.
 - <https://www.arin.net/resources/manage/rpki/rpa.pdf>
- Repository Quality
 - RPKI provides repository integrity / authentication.
 - **Repository availability needs to be measured.**
- Transformation / Distribution
 - RPKI to RPSL for local use.
 - <https://blog.apnic.net/2018/08/01/treating-rpki-roas-as-irr-route6-objects/>
 - RPKI to JSON to CDN to scale distribution, ensure consistency.
 - <https://blog.cloudflare.com/cloudflares-rpki-toolkit/>
 - RPKI + BMP + Kafka for OV in data centers
 - <https://sites.google.com/site/amitsciscoz-one/home/networking-datascience/bgp-prefix-origin-validation-without-rpki-in-datacenter-networks>



Information Infrastructure Properties

• Data Consumers

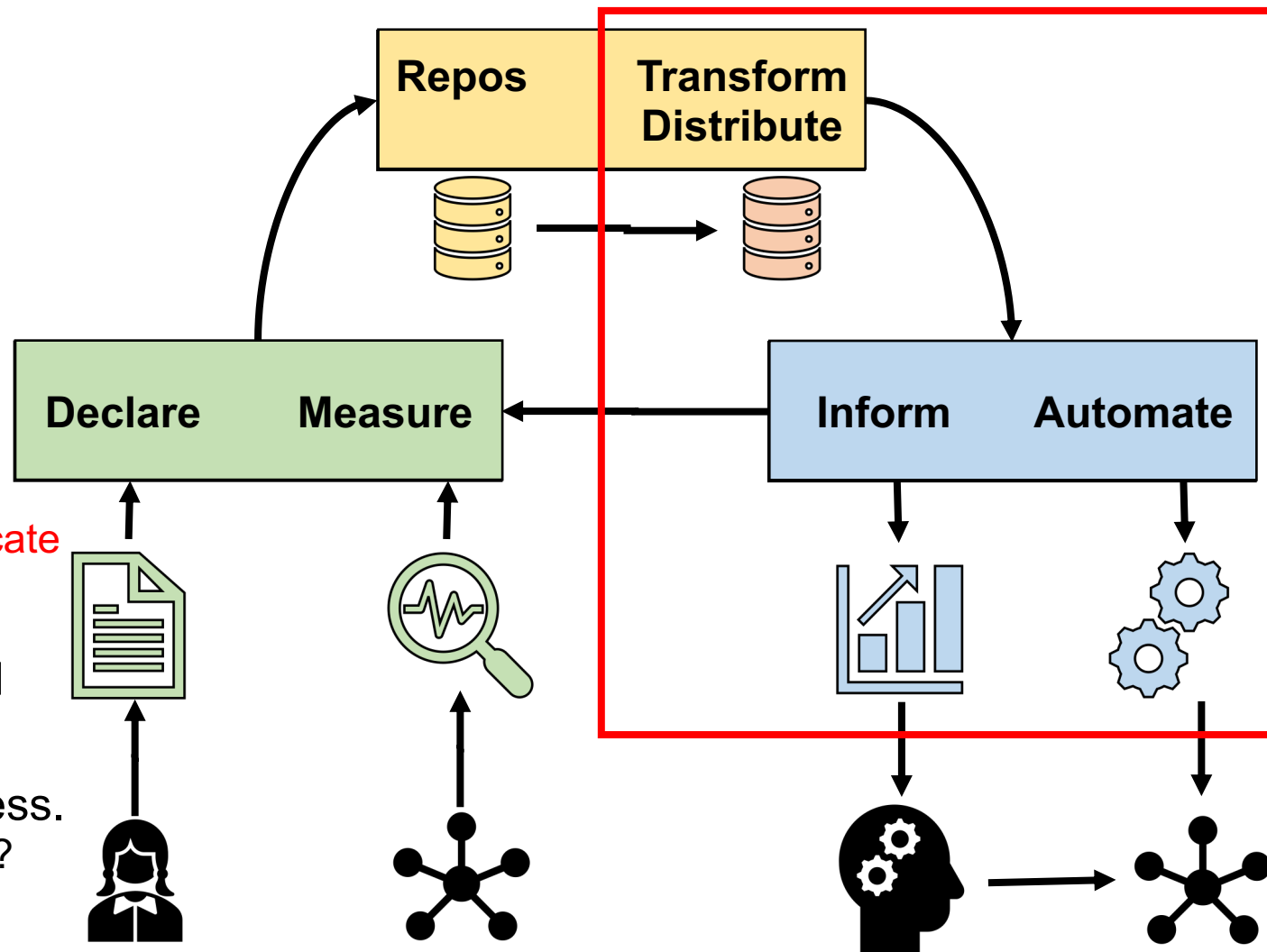
- Access control & Authentication
 - Who / what can access data?
 - How do you verify above?
- Information Quality
 - Meta data for completeness, correctness, uncertainty?
 - Meta data for information provenance?
- Responsiveness / Liveness
 - Repository change to automated change to control/data plane or alert?



Information Infrastructure Properties

• Data Consumers

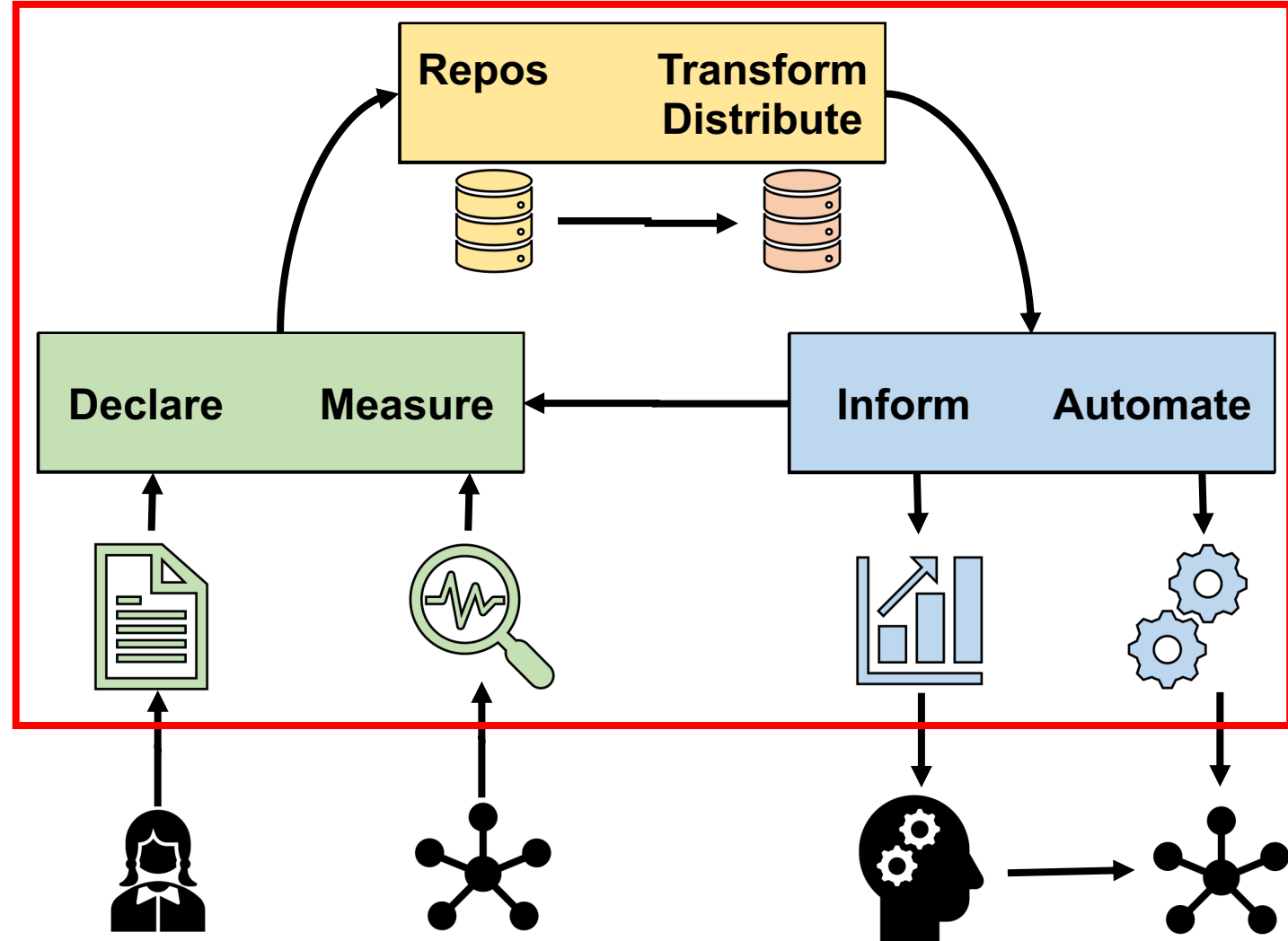
- Access control & Authentication
 - ARIN – RPA to access TAL, otherwise open and unauthenticated access.
- Information Quality
 - Meta data for completeness, correctness, uncertainty?
 - Meta data for information provenance?
 - RPKI ROAs/CERTs do not indicate who created them?
- Responsiveness / Liveness
 - Repository change to automated change to control/data plane or alert?
 - End to end system responsiveness.
 - E.g., Reactive DDoS mitigation?



Information Infrastructure Properties

• Other Operational Issues

- Incremental Deployment and Phased Adoption
 - Can producers control which consumers use the data?
 - Can producers influence how consumers use data?
 - **Soft launch – flag and report?**
- Monitoring Information Use.
 - Can producers monitor consumers' behavior?
 - Who is using the information and how?
 - **Standardized behavior / use?**
- Systemic Risk Issues
 - Risk of compromise / failure of each component?
 - Ability to diagnose problems?
 - Behavior at scale?



RPKI Monitoring Tools

NIST RPKI Monitor(s)

• <https://rpki-monitor.antd.nist.gov/>

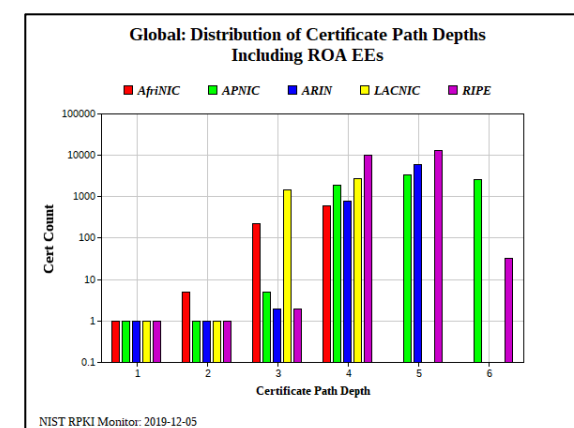
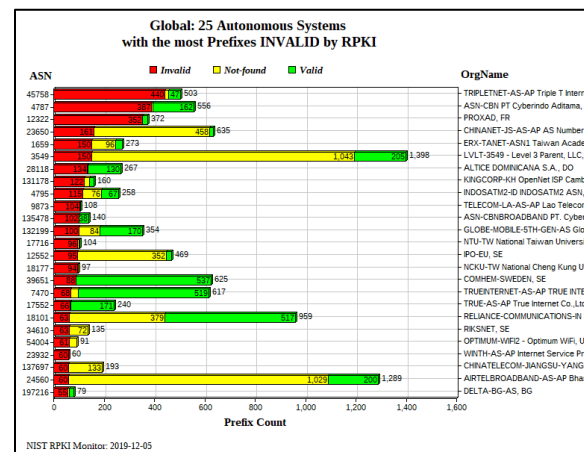
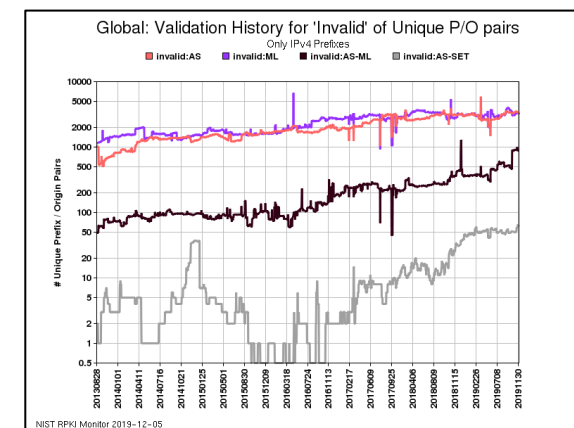
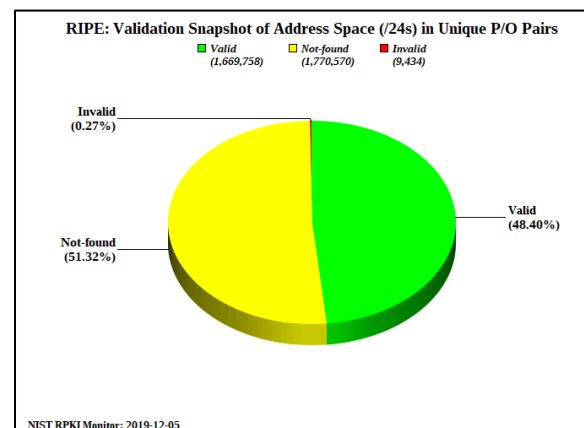
• Running since ~2013

• Status of RPKI adoption

- Relative to BGP – Origin Validation
 - Analysis of RPKI relative to BGP Data.
 - Analysis of apparent issues.
 - Tracking adoption trends – good and bad.
 - Global / per region statistics.

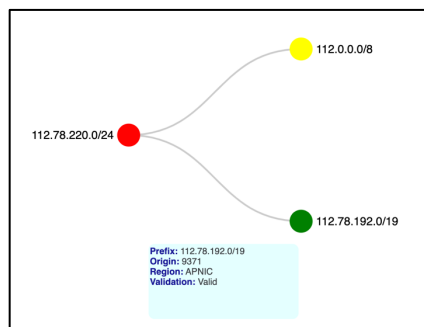
• Analysis of RPKI Data – size / shape

- Understand RPKI usage per region
 - Mainly how the RIR hosted RPKI data sets compare



New RPKI Monitor

- <https://coming.soon> :^)
- **New focus / capabilities**
 - Focus on identifying significant changes
 - Being able to correlate change in OV to change in RPKI.
 - Being able to understand potential routing impact of such changes.
 - Email / twitter feeds to alert users when there is something of interest



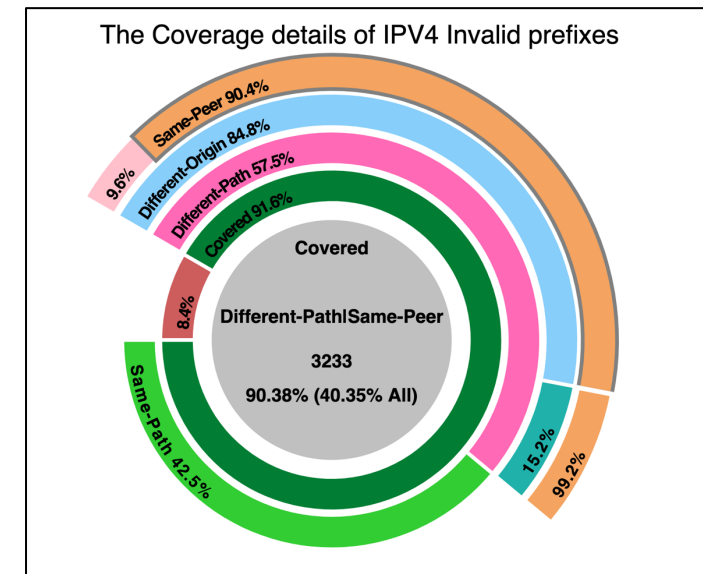
Latest RPKI-Validation changes (From 2019-12-09:12 To 2019-12-09:18)

IPv4 RPKI Origin Validation Changes

Number of changes :	47	100%
Not-Found to Valid :	43	91.49%
Not-Found to Invalid :	2	4.26%
Valid to Invalid :	1	2.13%
Invalid to Valid :	1	2.13%

IPv6 RPKI Origin Validation Changes

Number of changes :	8	100%
Not-Found to Valid :	5	62.50%
Invalid to Valid :	3	37.50%



NIST ITL RPKI-ROV Analysis

ORIGIN	PREFIX	COUNT	TIME	VALIDATION	ROAs (2019-08-12-19)			ROAs (2019-09-12-19)		
					Prefix1	Origin1	ML1	Prefix2	Origin2	ML2
20473	103.144.88.0/24	1	[2019-12-06:18, 2019-12-09:00]	Valid to Invalid:AS	103.144.88.0/24	20473	24	103.144.88.0/24	139734	24
46887	207.237.156.0/23	1	[2019-12-09:06, 2019-12-09:12]	Valid to Invalid:AS	207.237.156.0/23	46887	23	-	-	-
-	-	-	-	-	-	-	-	207.237.0/16	6079	24
47065	147.28.241.0/24	2	[2019-12-06:18, 2019-12-09:00]	Valid to Invalid:AS	147.28.241.0/24	47065	24	147.28.241.0/24	51224	24
-	-	-	-	-	-	-	-	147.28.0/16	3130	16
-	-	-	[2019-12-09:06, 2019-12-09:12]	Invalid:AS to Valid	147.28.241.0/24	51224	24	147.28.241.0/24	47065	24
-	-	-	-	-	147.28.0/16	3130	16	-	-	-

New RPKI Monitor

- **Explore validation history**
 - Examine validation history of a prefix.
 - Correlate OV changes to RPKI data.
 - Drill down into RPKI certs at chosen point in time.

```

» apnic-rpki-root-iana-origin.cer
  » mBQsnQtBo7n7YD12mEgjb9HzGSQ.cer
    » DmWk9f02tb1o6zySNAiXjJB6p58.cer
      » 50RvIPODPmrPyWmaRmG2QnJ5Lw.cer
        » 9CCC398A194111EA9DC3274AC4F9AE02.roa
  
```

FileName	9CCC398A194111EA9DC3274AC4F9AE02.roa
ASN	AS139734
Validity Period	2019-12-07T22:53:47.000Z - 2021-01-31T00:00:00.000Z
Signing Time	2019-12-07T22:53:47.000Z

Prefix	Max length
103.144.88.0/24	24
2001:df1:b980::/48	48



ROAs for Prefix 103.144.88.0/24 Originated from 20473

	Origin	Prefix	Max Length	Time
Valid	20473	103.144.88.0/24	24	2019/12/1:0 - 2019/12/3:12
Valid	20473	103.144.88.0/24	24	2019/12/3:18 - 2019/12/4:12
Valid	20473	103.144.88.0/24	24	2019/12/4:18 - 2019/12/5:0
Valid	20473	103.144.88.0/24	24	2019/12/5:6 - 2019/12/5:18
Valid	20473	103.144.88.0/24	24	2019/12/6:6 - 2019/12/6:18
Invalid:AS	139734	103.144.88.0/24	24	2019/12/8:18 - 2019/12/9:18

Questions and Discussion

- **For more information:**

- Robust Interdomain Routing Project
 - <https://www.nist.gov/programs-projects/robust-inter-domain-routing>
- Advanced Network Technologies Division.
 - <https://www.nist.gov/itl/antd>
- Information Technology Laboratory
 - <https://www.nist.gov/itl>

