BIOTEAM
Accelerate Science

Authorization (AuthZ) Engine Architecture for Distributed Systems

John Jacquay

Senior Scientific Systems Engineer

What is AuthZ?

Authorization Answers Questions Like:

- What information or resource(s) does the **{ subject }** have access to?
- Is the **{ subject }** permitted to perform **{ operation }** on this **{ resource }**?

BIOTEAM
Accelerate Science

Physical Realm AuthZ

- Mailboxes!
  - Key & lock is AuthN
  - Boxes and rear door as AuthZ
- A house with no AuthZ
- What about data systems?

Why do we care about AuthZ in data systems?

- In the physical realm, authorization is well understood
- Ensures: confidentiality, integrity, and availability of resources
- Protects resources
  - Reduce impact of bad actors
  - Can protect PHI data or EMRs
- Create chains of trust
- Exert control over systems

BIOTEAM
Accelerate Science

Why Do I Care? Because **Data == Power**

Intelligence ⟺

Data ->

Knowledge ->

Patterns / Trends ->

Prediction ->

Control ->

Influence & Power

BIOTEAM
Accelerate Science

Intellegence in Climate: Hot or Not?

"It's **cold** outside **today**, the climate isn't getting warmer"

"It's cold outside today, however, the trends in data point to a **warmer climate**"

Disconnected Data Points

Connected Data Points

BIOTEAM
Accelerate Science

Intelligence In Warfare: Victory or Defeat?

BIOTEAM
Accelerate Science

Intelligence In Therapeutics: Profit or Loss?

WHO WOULD WIN?

Psilocybin N=30
25mg / **every 3 weeks**
QIDS-SR-16 score: **-8.0** +/- 1.0

Escitalopram N=29
10mg / 20mg / **every day**
QIDS-SR-16 score: **-6.0** +/- 1.0

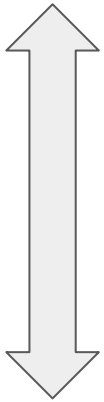
(2021) Trial of Psilocybin versus Escitalopram for Depression - .N Engl J Med 2021; 384:1402-1411
https://www.nejm.org/doi/full/10.1056/nejmoa2032994

BIOTEAM
Accelerate Science

History of AuthZ Strategies

- **Club Bouncer:** Bruce
- **Unix:** File/directory permission bits
- **ACL:** Access Control List
- **RBAC:** Role-Based Access Control
- **ABAC (PBAC):** Attribute-Based Access Control
- **RAdAC:** Risk Adaptive-Based Access Control

Simple,
Less Expressive,
Less Sophisticated

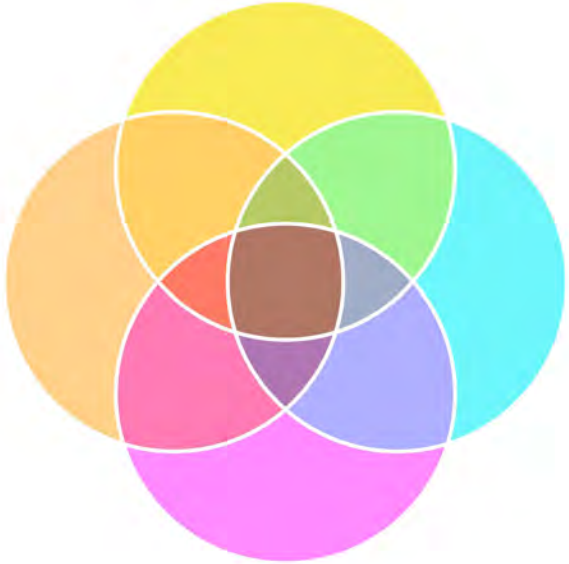


Complex,
More Expressive,
More Sophisticated

BIOTEAM
Accelerate Science

Other Access Control Mental Models

- **MAC** - Mandatory Access Control
  - Centrally managed
  - Permissions governed by identity + object tags (sensitivity)
  - e.g. Military and intelligence community governance
- **DAC** - Discretionary Access Control
  - Decentralizes security decisions to resource **owners**
  - Permissions governed by identity
  - e.g. Unix permissions, ACLs, etc…



BIOTEAM
Accelerate Science

History of AuthZ Strategies: ACL

- ACL: Access Control List
- More granular and flexible

control— versus linux file mode bits

```
# file: home/sales/
# owner: john
# group: john
user::rw-
user:barryg:r--
group::r--
mask::r--
other::r--
default:user::rwx
default:user:john:rwx
default:group::r-x
default:mask::rwx
default:other::r-x
```

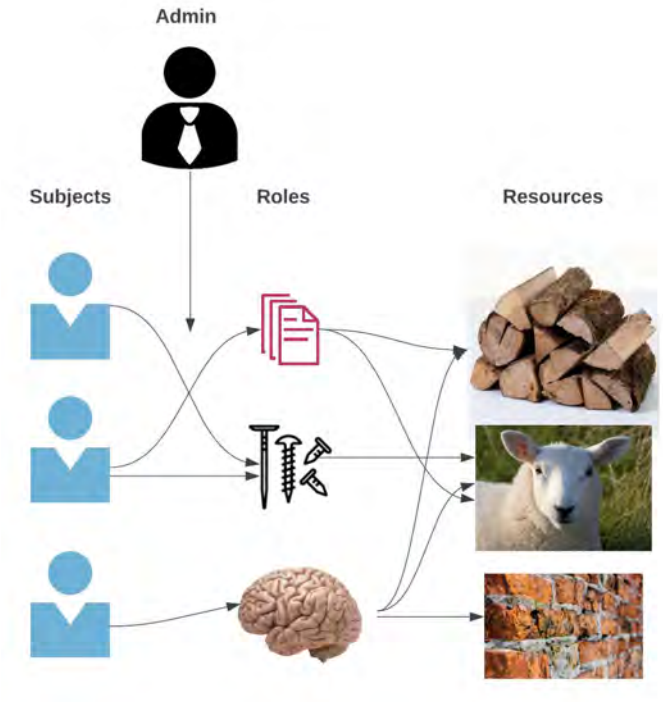
BIOTEAM
Accelerate Science

History of AuthZ Strategies: RBAC

RBAC:

Role-Based Access Control

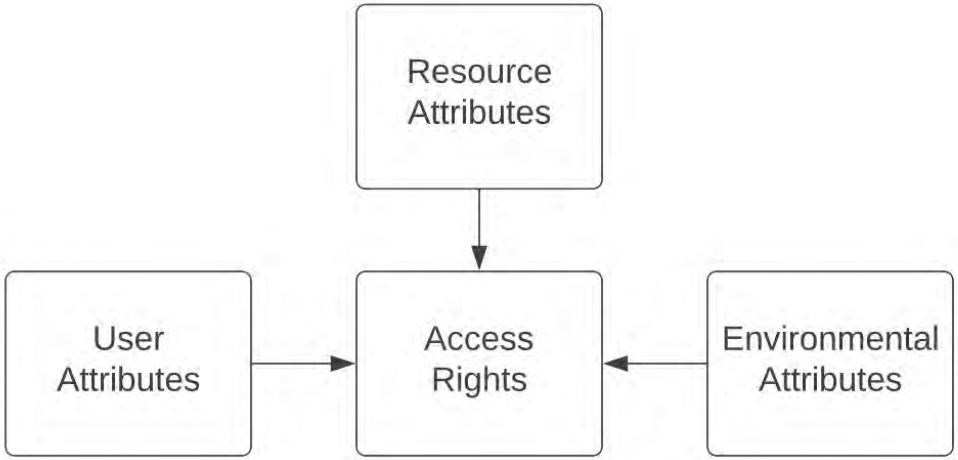
Subjects ->
Roles ->
Resource Permissions



BIOTEAM
Accelerate Science

History of AuthZ Strategies: ABAC (PBAC)

ABAC (PBAC):
Attribute-Based Access Control



BIOTEAM
Accelerate Science

History of AuthZ Strategies: RAdAC

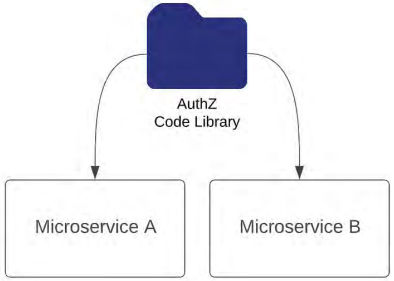
RAdAC: Risk Adaptive-Based Access Control

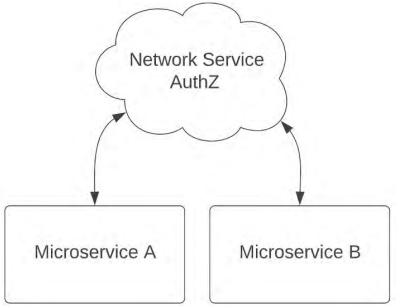
- Examples:
  - To gain access to the conference, you must have a negative COVID test within the last 24 hours
  - You must not have visited a country with a breakout of virus x within the last 5 years
  - You must fly on an airline that meets our constantly changing requirements
- Difference from ABAC? Takes risk assessments to the extreme
  - Subject, resource, and environmental variables as knowledge graph, even utilizing external data sources
- Good place for application of AI/ML models that learn risks

BIOTEAM
Accelerate Science

History of AuthZ Architecture

Ad Hoc -> **Shared Libraries** -> **Network Service**





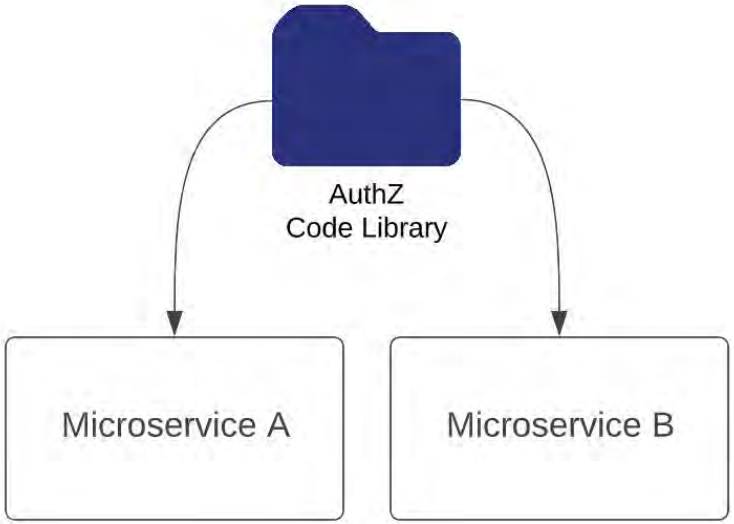
BIOTEAM
Accelerate Science

Architecture: Ad-Hoc

- Any AuthZ strategy
- Do whatever you want!
- Tightly coupled with application code and logic
- Service-specific
  - Not applicable to other services

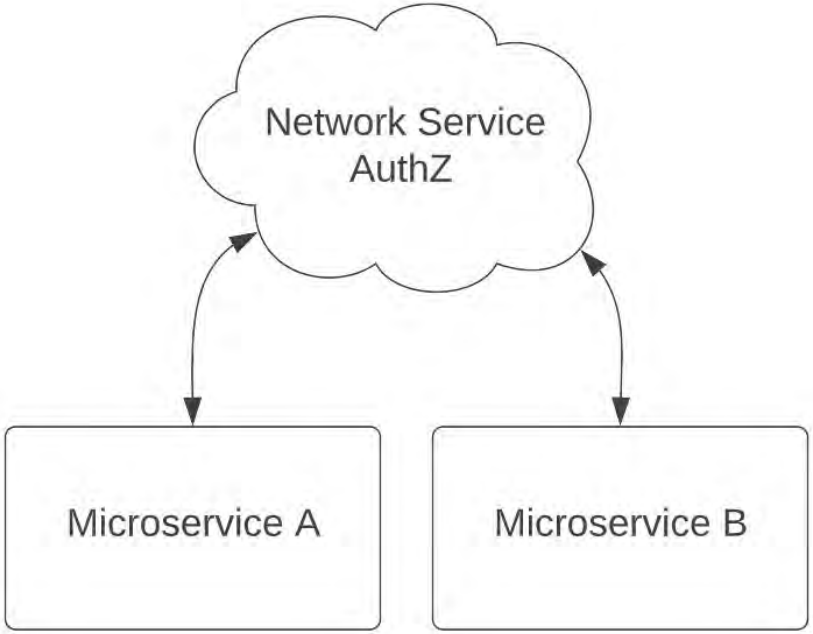
BIOTEAM
Accelerate Science

Architecture: Shared Library



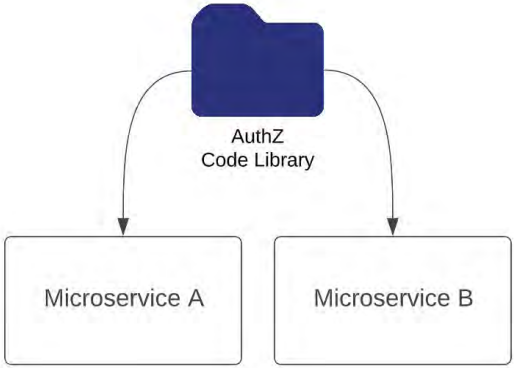
BIOTEAM
Accelerate Science

Architecture: Network Service

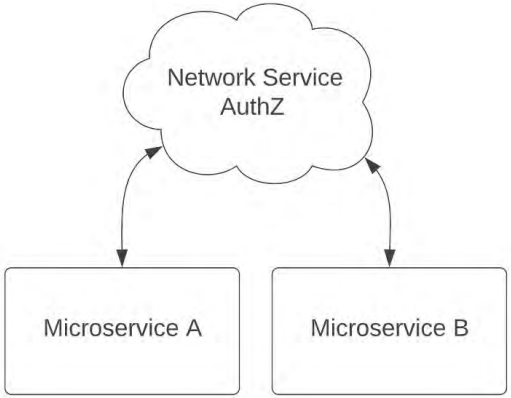


BIOTEAM
Accelerate Science

Architecture: Hybrid?



+



= ?

BIOTEAM
Accelerate Science

Common Problems in AuthZ Systems

- Not able to express governance at a level of granularity required
- Not able to fully express required logic and rules for access
- Slow || Doesn't scale
- Not readily interoperable

BIOTEAM
Accelerate Science

Distributed AuthZ Engine Proposal

John's Tenets & Principles of a Good One™

Just Remember:

M S C S C D

BIOTEAM
Accelerate Science

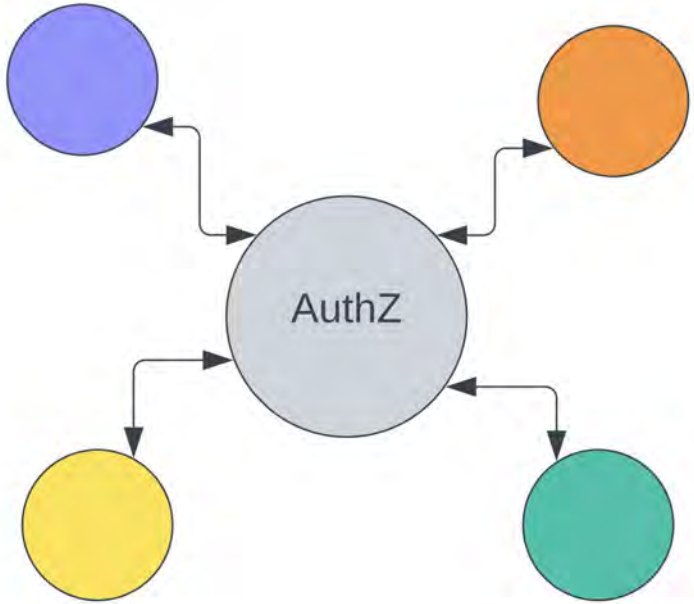
Principles & Tenets of a Good, Distributed, AuthZ Engine

- **M**ultimodal: Orchestrate AuthZ governance for multiple services
- **S**calable
- **C**ryptographically trustable, correct, and consistent
- **S**upports advanced logic and capabilities
- **C**ommon syntax and vocabulary to define governance rules
- **D**ecoupled and modular, yet connected with mutually understood logic

BIOTEAM
Accelerate Science

Multimodal: AuthZ Governance for Many Services

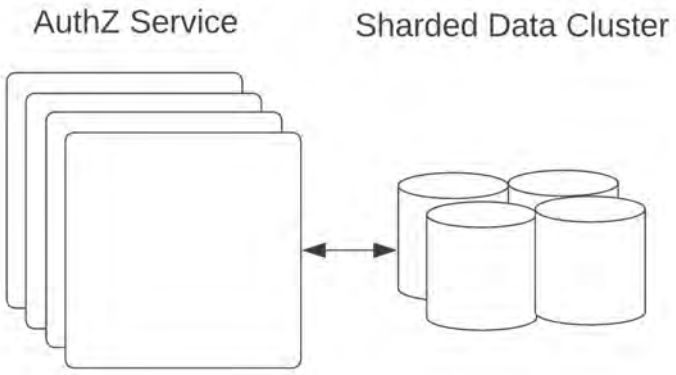
- Protects many types of resources from various services
- AuthZ engine runs as a decoupled network microservice
- Implementation should be generic and polymorphic
- Easily add or remove a service



BIOTEAM
Accelerate Science

Scalable

- Able to serve a high volume of requests and rules
- Implies denormalized data at some point
- Informs the architecture of the infrastructure



BIOTEAM
Accelerate Science

Cryptographically Trustable, Correct, and Consistent

- Signed claims to reduce required communication
  - JWT
  - Why? No need for client to ask multiple times
- TLS to ensure authentication, integrity, and privacy

BIOTEAM
Accelerate Science

Supports Advanced Capabilities

- ABAC or RAdAC level logic complexity
- Permissions for the data are determined by the data itself, connections to external data, or connections to the subject
  - and the relationships within resource data

BIOTEAM
Accelerate Science

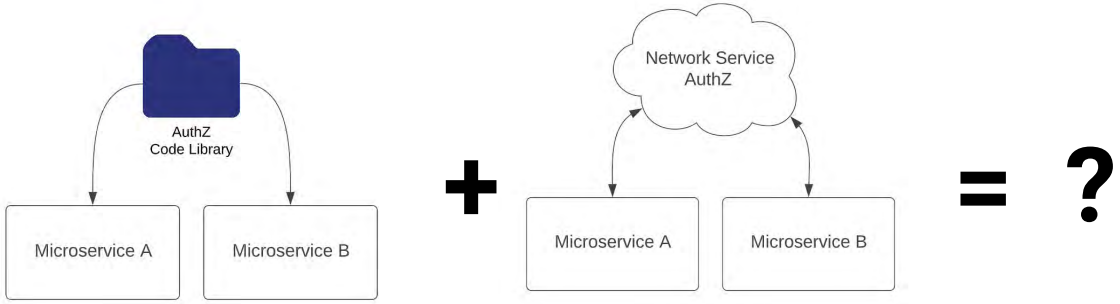
Common Syntax and Lexicon to Define Governance Rules

- Declarative, not imperative
  - YAML or JSON
  - Custom DSL - Ruby would be great for this
  - Better for developing GUIs and for use by non-coders
- Common logic and behavior well abstracted and reusable
  - Use them as to not reinvent the wheel or produce Wet markup or code

BIOTEAM
Accelerate Science

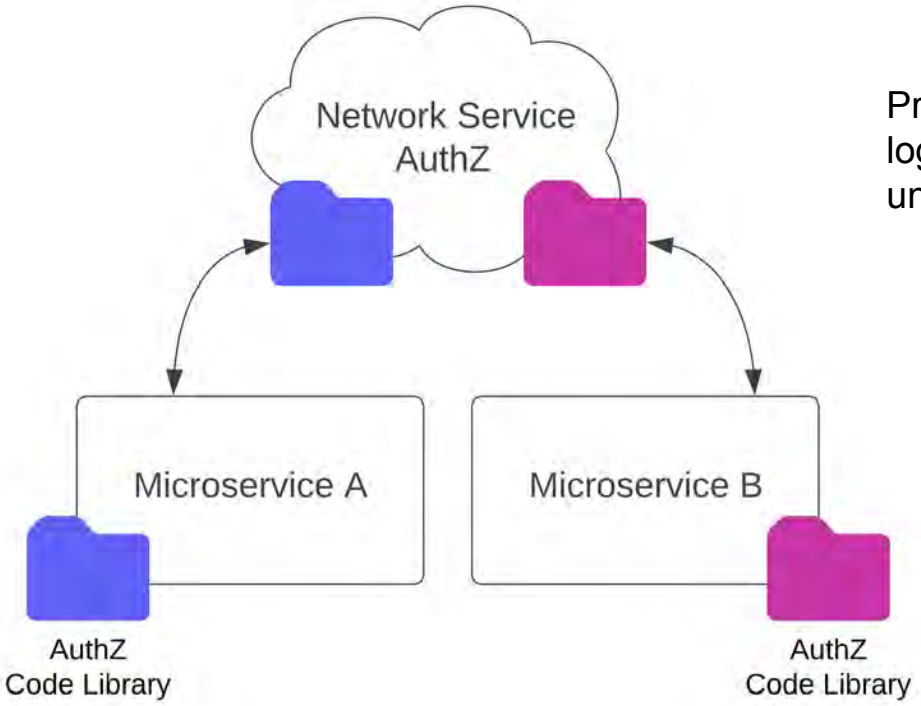
Decoupled and Modular, yet Connected with Mutually Understood Logic

- Boolean responses versus more nuanced responses and policy— The annoying subordinate problem
- Merging of shared library and network service architectures



BIOTEAM
Accelerate Science

Hybrid: Network service w/ shared libraries



Protected resources and business logic permissions/policy shared and understood

BIOTEAM
Accelerate Science

The Annoying Subordinate Problem

```
while ( true ) {
    prompt("Can I have a cookie?")
}
```

```
while ( true ) {
    prompt("Can I put this expense on my report?")
}
```

BIOTEAM
Accelerate Science

The Annoying Subordinate Problem

Empower the requestor to make decisions using a well defined policy.
The requestor must be trusted to adhere to the policy.

prompt("Can I have a cookie?")

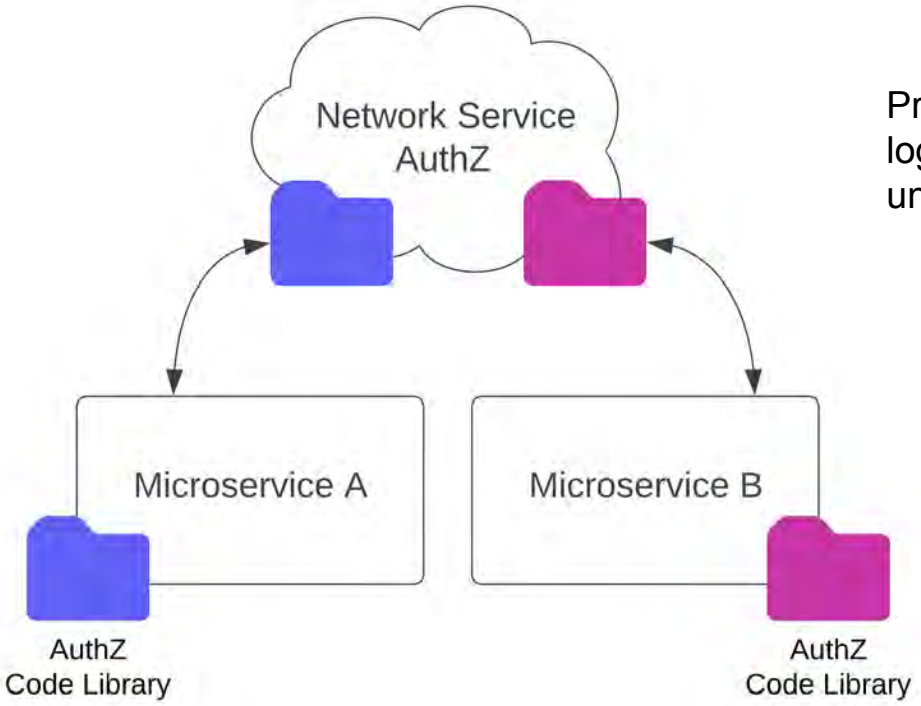
// yes, but it must be after you've eaten your dinner and it must be an oatmeal raisin cookie

prompt("Can I put this expense on my report?")

// Please stop asking me. You're using all of my time and energy to answer these questions. Please refer to the employee handbook for our policy on approved expenses

BIOTEAM
Accelerate Science

Hybrid: Network Service with Shared Libraries



Protected resources and business logic permissions/policy shared and understood

BIOTEAM
Accelerate Science

Players in the Game

- Google Zanzibar
  - https://github.com/ory/keto
  - https://github.com/authzed/spicedb
  - https://github.com/authorizer-tech/access-controller
- Cloud provider IAM
- Gen3's Arborist
- BioTeam!

BIOTEAM
Accelerate Science

Underlying Rule/Claim Transport Formats

XACML

JWT

PASETO

Open Information and Open Code

John believes the democratization of information and code:

Open

Accessible

BIOTEAM
Accelerate Science

With Great Power, Comes Great Responsibility

- Responsibility is bidirectional: between the actors, and governance

- AuthZ shouldn't be used to restrict and oppress, should be used to protect

BIOTEAM
Accelerate Science

Zero Sum Game

	Choice 1	Choice 2
Choice 1	–A, A	B, –B
Choice 2	C, –C	–D, D

Generic zero-sum game

BIOTEAM
Accelerate Science

The End

Thanks For Listening!

BIOTEAM
Accelerate Science