AXIOMATICS

Identity Solved. What Next?

Tackling your Toughest Authorization Challenges

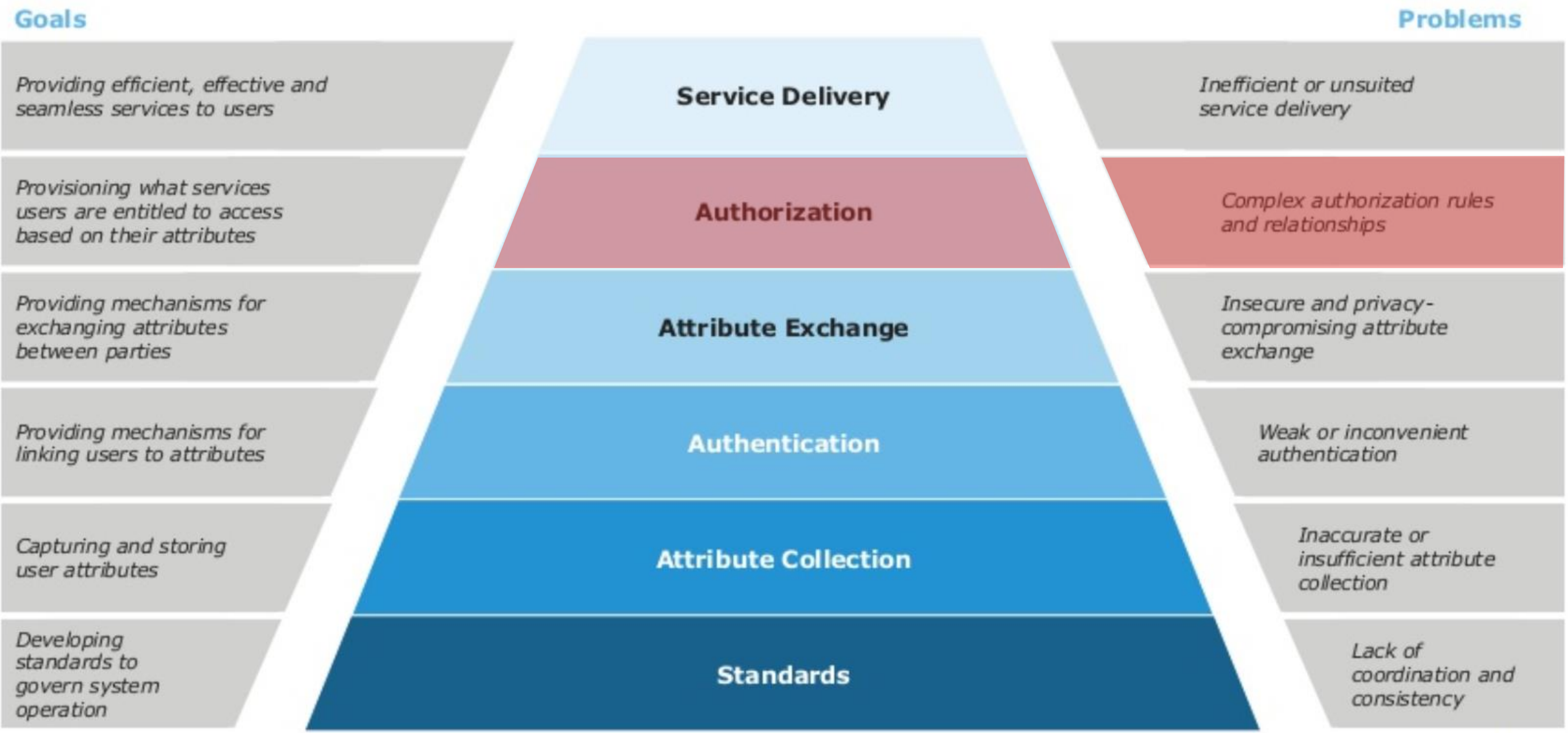
May 17th 2018

David Brossard

On the internet ~~no one~~ ***everyone*** knows you’re a dog

© Axiomatics 2018 - All Rights Reserved

A Blueprint for Digital Identity[1]



Goals
Problems
Providing efficient, effective and seamless services to users
Service Delivery
Inefficient or unsuited service delivery
Provisioning what services users are entitled to access based on their attributes
Authorization
Complex authorization rules and relationships
Providing mechanisms for exchanging attributes between parties
Attribute Exchange
Insecure and privacy-compromising attribute exchange
Providing mechanisms for linking users to attributes
Authentication
Weak or inconvenient authentication
Capturing and storing user attributes
Attribute Collection
Inaccurate or insufficient attribute collection
Developing standards to govern system operation
Standards
Lack of coordination and consistency

[1] From A blueprint for digital identity, Christine Robson, Deloitte, Cloud Identity Summit 2017.

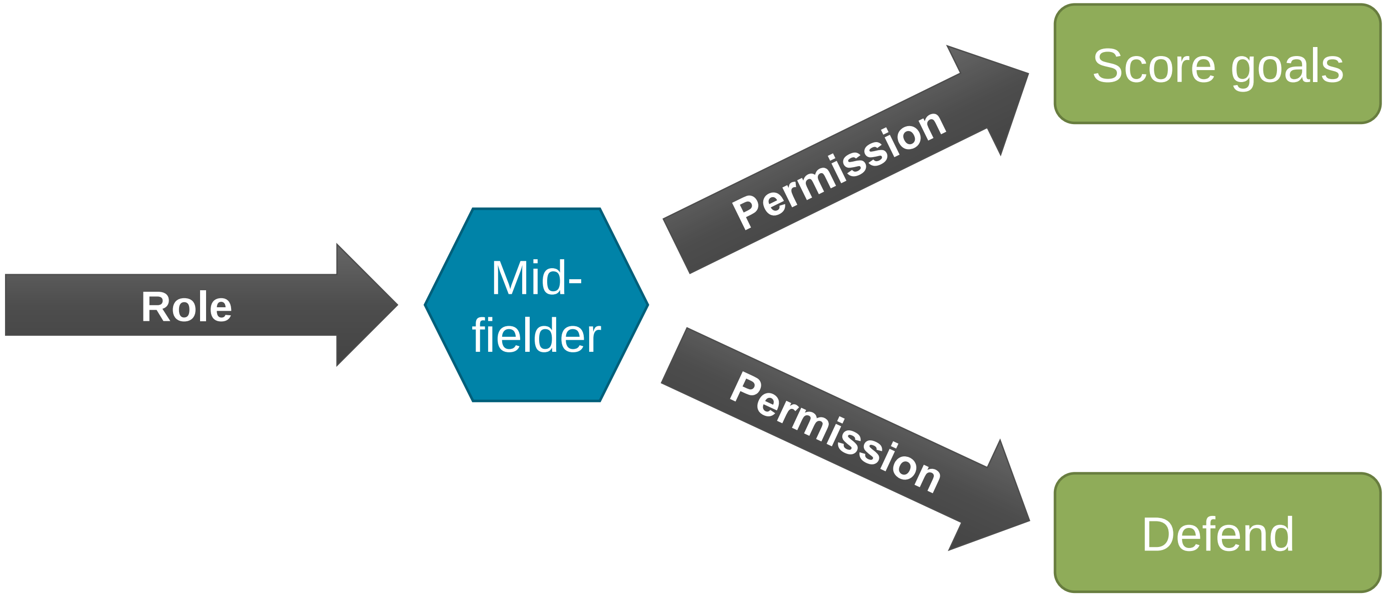
Authorization is about letting the *right one* in

Access Control Lists (ACL)

AXIOMATICS

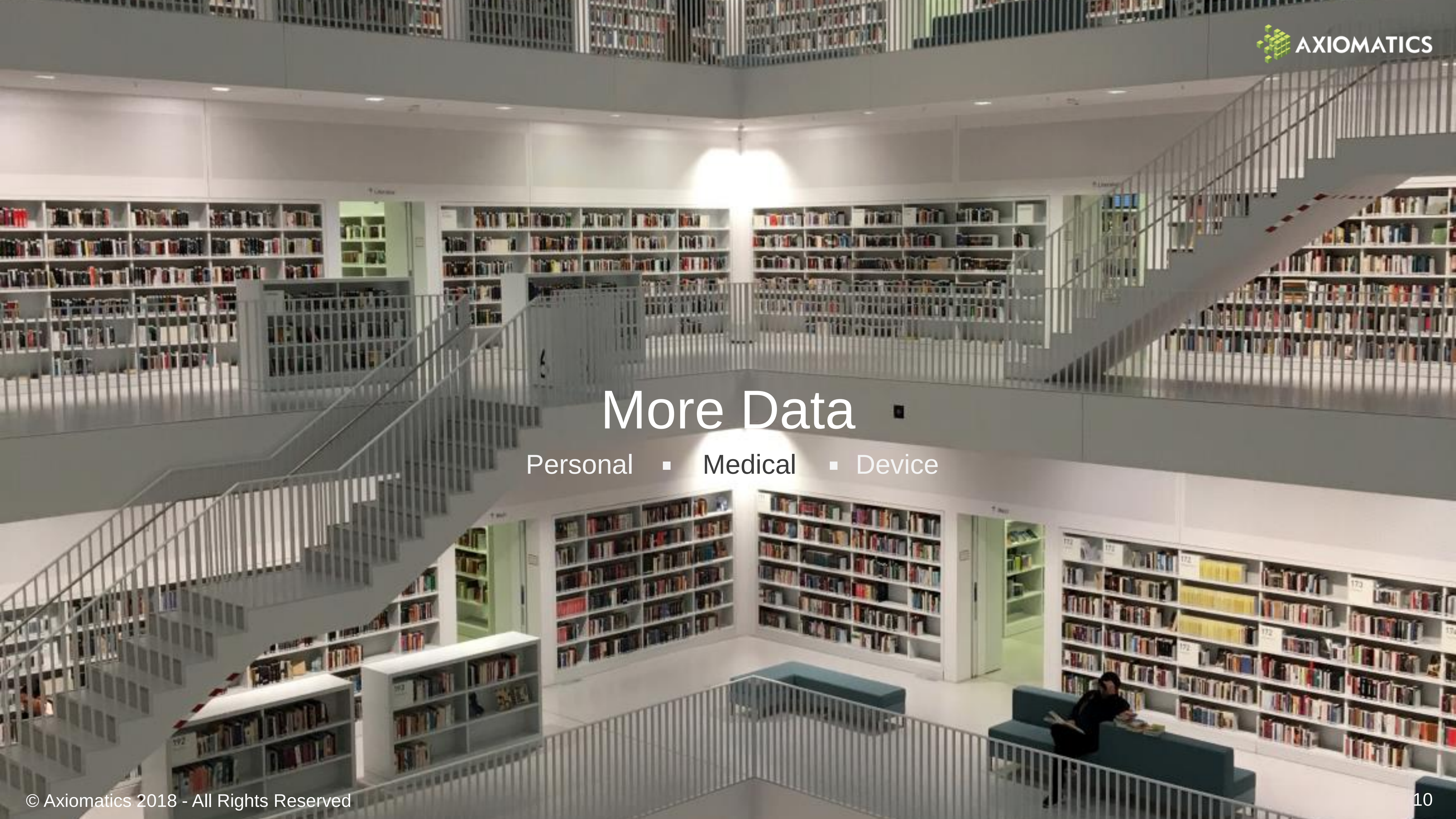
And 19[illegible]pened…

RBAC to the rescue



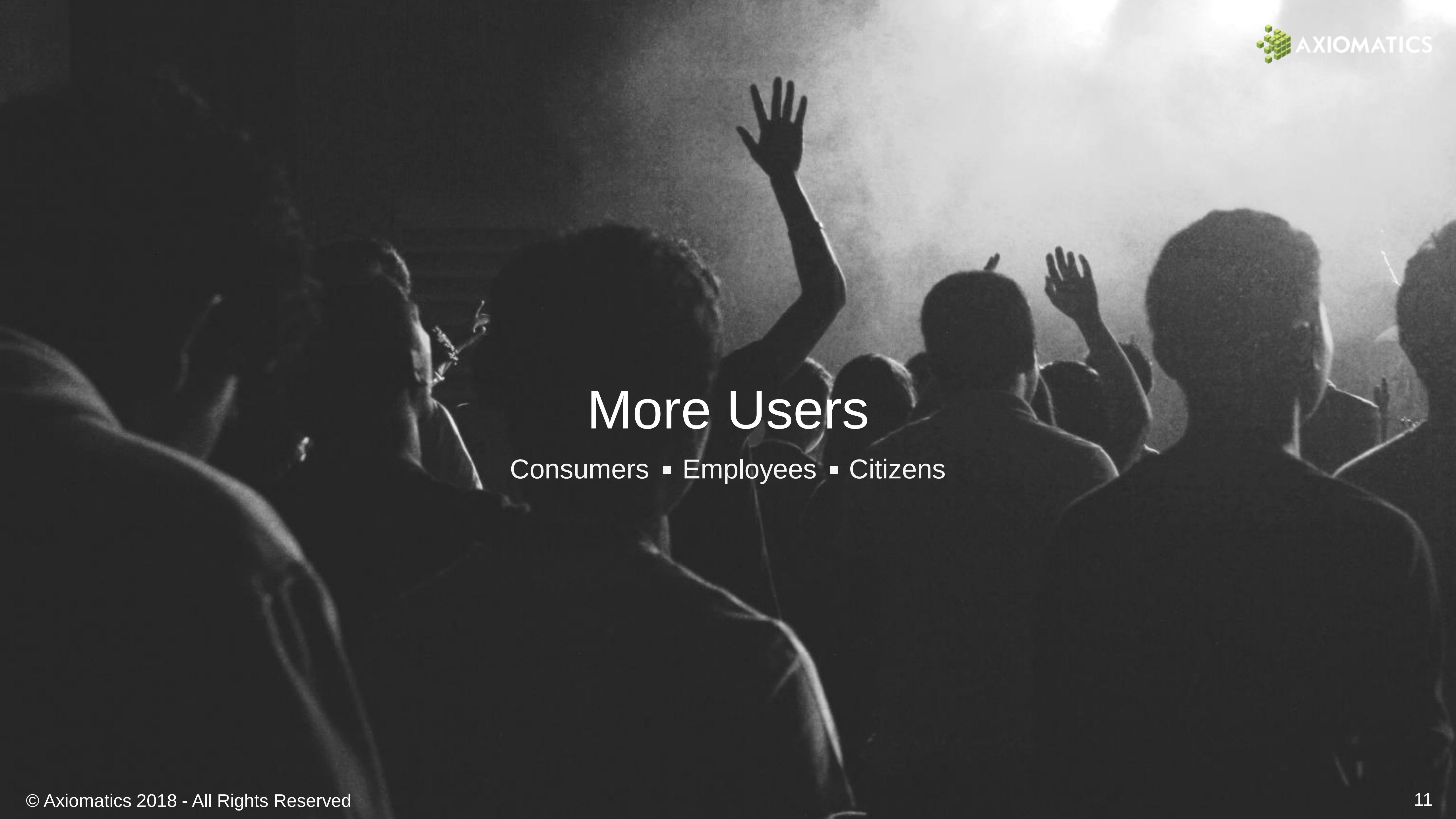
Let’s Fast-forward to Today

Every Company is a ***Software*** Company



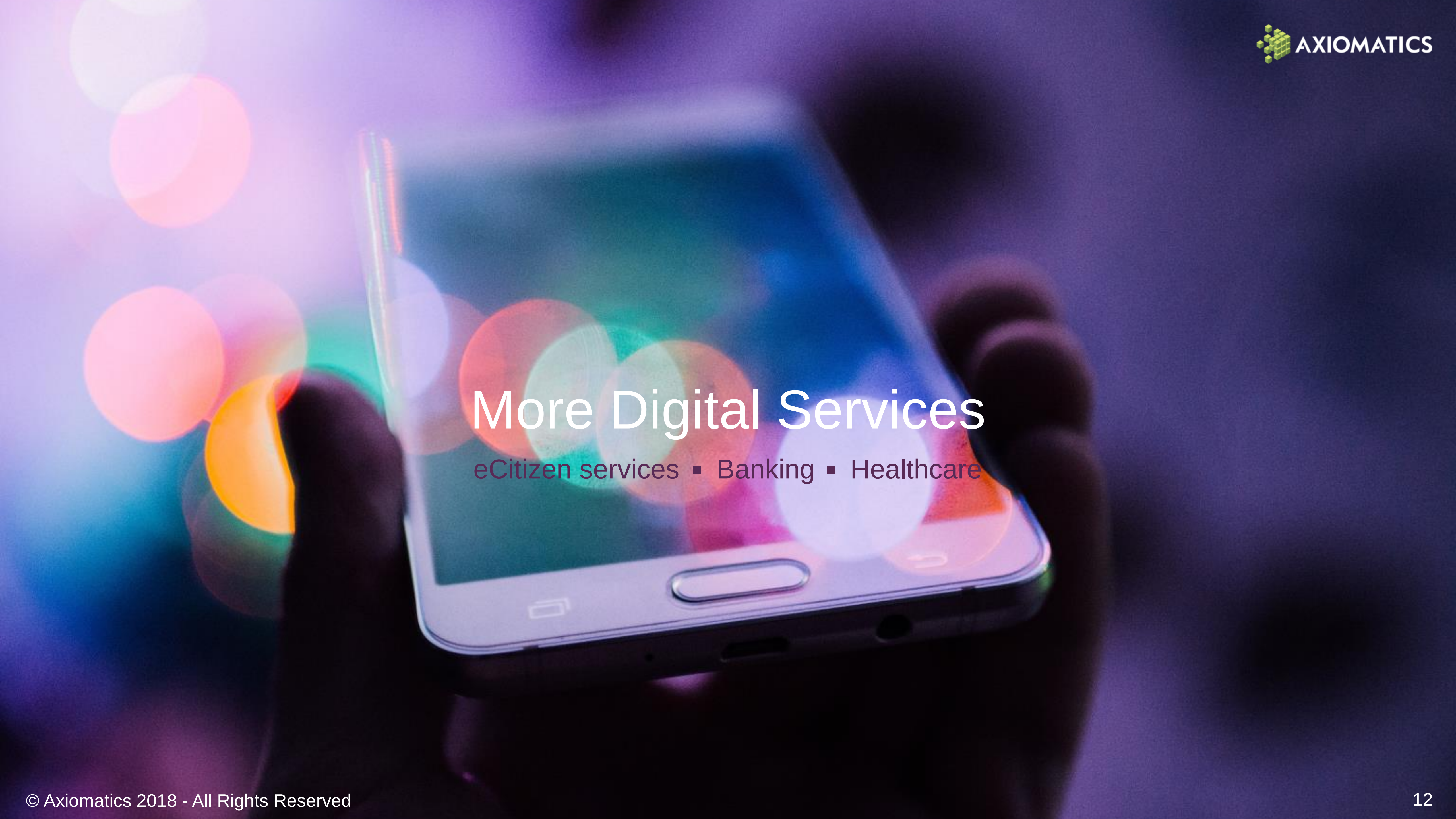
More Data

Personal ▪ Medical ▪ Device



More Users

Consumers ▪ Employees ▪ Citizens



More Digital Services

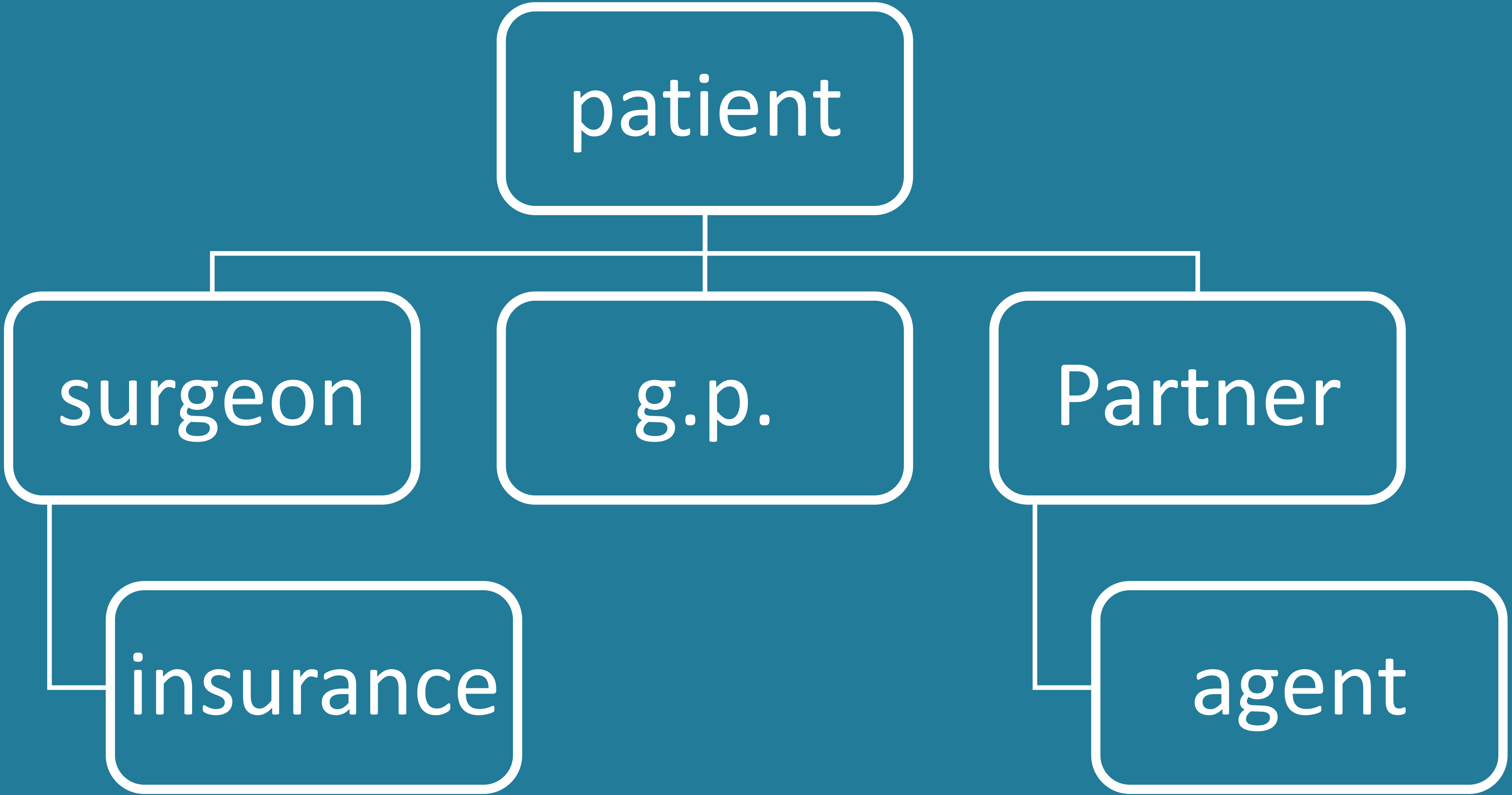
eCitizen services ▪ Banking ▪ Healthcare

RBAC Does Not Scale

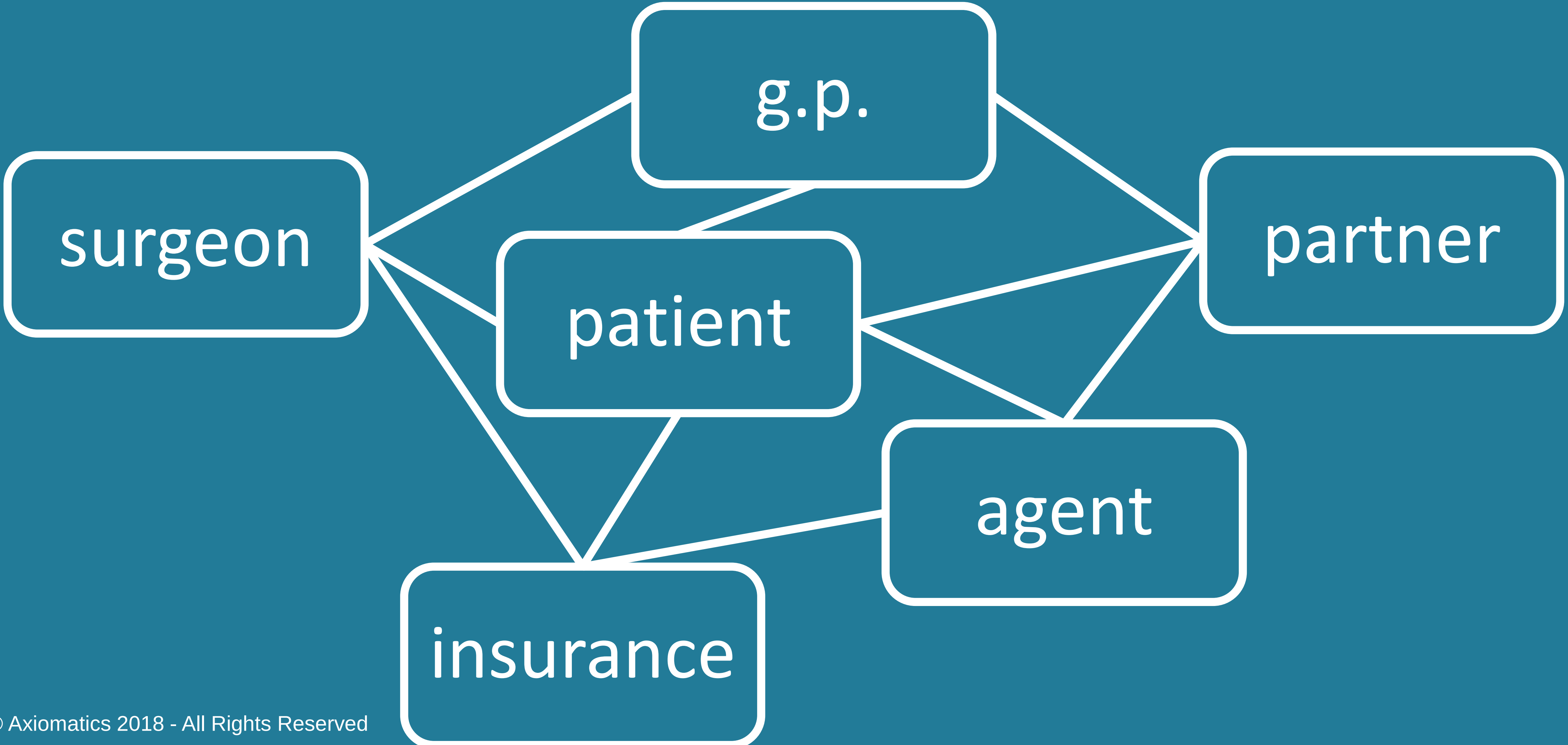
Role explosion ▪ Stale permissions ▪ Toxic combinations

Existing Approaches are too *Ego*centric

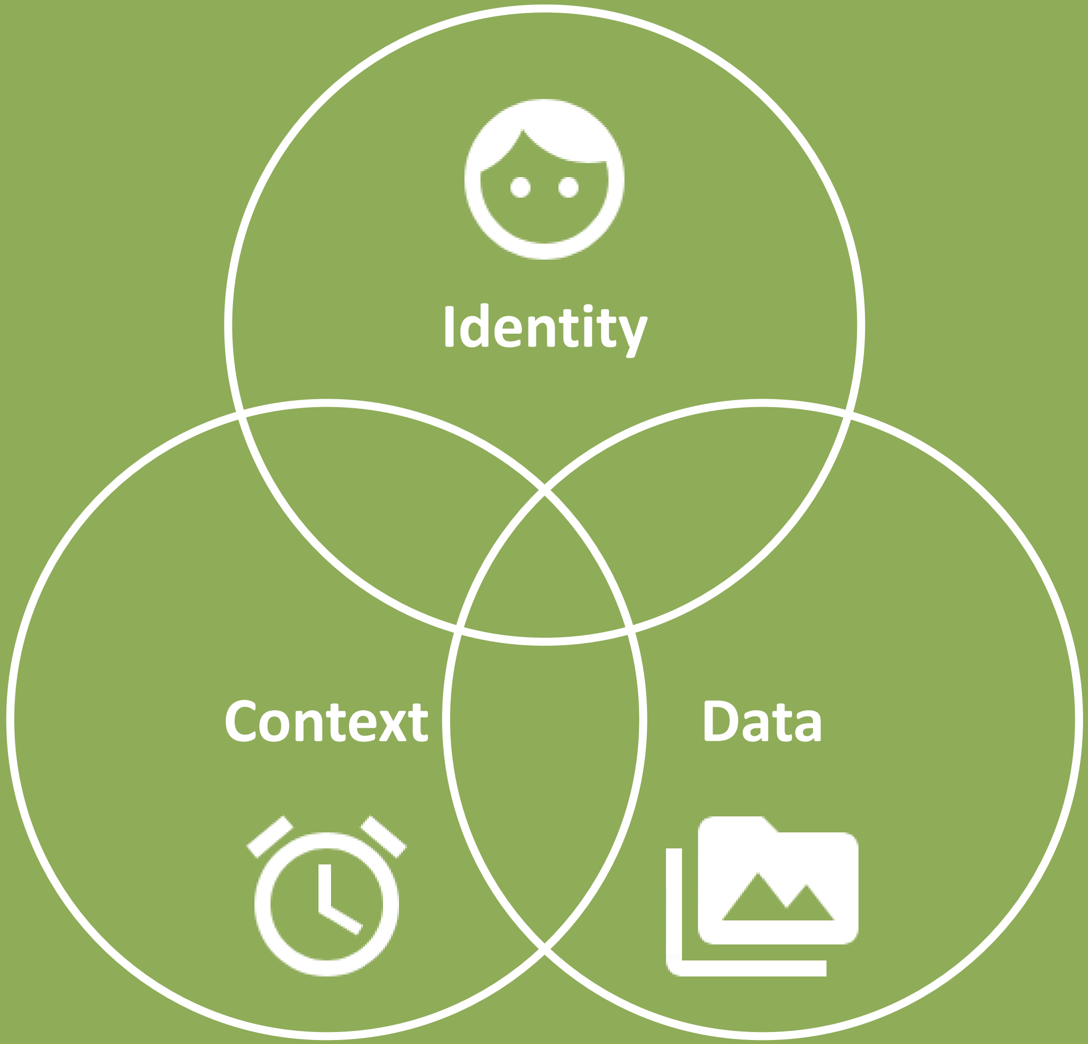
The World According to RBAC & LDAP



The Real World: A Graph



The Venn of Dynamic Authorization Management



Identity

Context

Data

Attribute Based Access Control

Dynamic Authorization Management

Attribute ▪ Policy ▪ Graph ▪ Relationship

Attribute-Based Access Control

A context-aware and dynamic authorization model

Who? What? When? Where? Why? How?

time = “3:54pm”

location = “Kalamazoo”

device= “corporate”

vpn= true

Policies Tie in the Attributes

role = “manager”

department = “sales”

id= “Alice”

status= “active”

type = “purchase order”

department = “sales”

owner= “Alice”

amount= 500

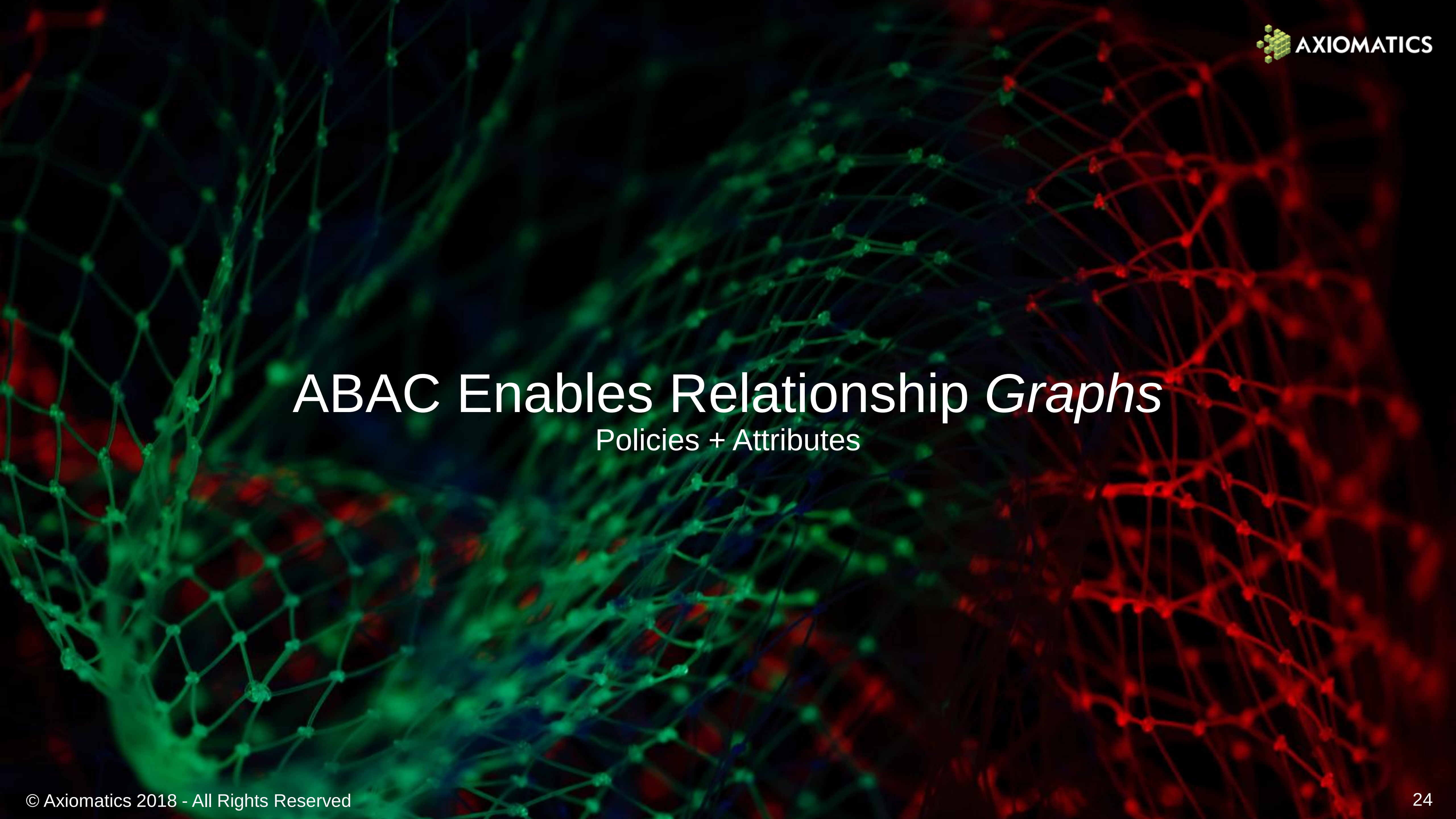
> “A user in the engineering department
> can view a blueprint
> If the parts are not export-controlled”

> “Active doctors
> can view medical records
> of patients assigned to them”

Policies are a Direct Reflection of Business Requirements

> “Managers in purchasing
> can approve purchase orders
> up to their approval limits”

ABAC Enables Identity Relationship Management



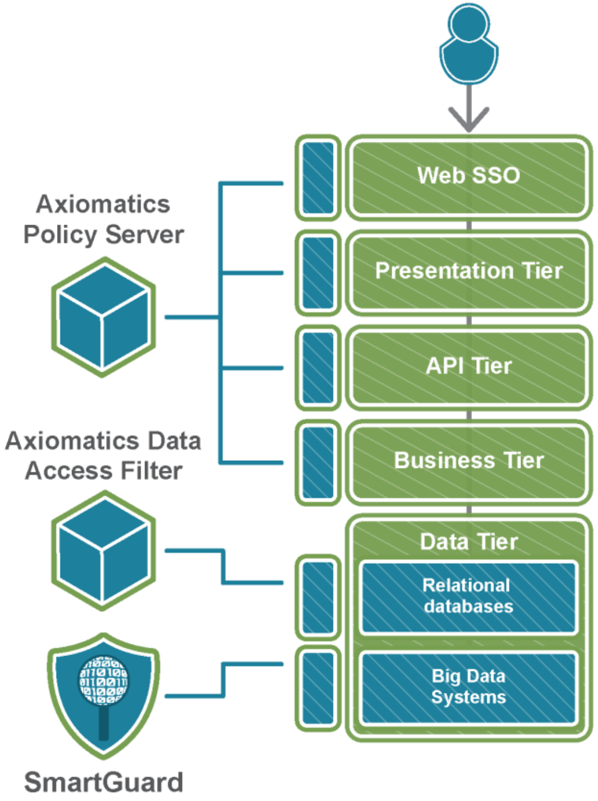
ABAC Enables Relationship *Graphs*

Policies + Attributes

Dynamic Authorization Management
=
Externalized Authorization Management

Externalized Authorization Management leads to

Any-Depth Authorization



Any-Breadth Authorization

- Comprehensive, 360° authorization
- On-premise and cloud
- Apps, APIs, microservices…
- SharePoint and other CMS
- ERPs e.g. SAP
- Relational databases
- Big Data

OAuth is Not Authorization

(It’s access delegation)

In Conclusion: Some Use Cases

- Securing online payments for 200 million users
- Securing exchange of clinical trial data in pharmaceutical research
- Millions of transactions a day secured for one of the world’ s largest banks
- Protecting privacy for insurance company’ s clients
- Compliance with Export Control regulations for aircraft manufacturers
- Copyright-protected streaming media for authorized users only
- Improving speed and quality of health IT systems for veterans nationwide