Tuebora
SELF DRIVEN IAM

Policy-driven IGA: Why this approach produces better outcomes?

Brian Iverson

31 May 2023

Identity Governance and Administration

Who’s working for whom?


Policy-based access control
Policy-driven administration

Brief Taxonomy Interlude

Identity Governance & Administration

Identities

Entitlements

Teams

Applications

=

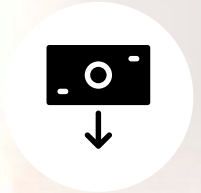
Accounts

Resources

Permissions

IT Systems

Finance & Accounting



Income

Expenses

=

Assets

Liabilities

Owners' Equity

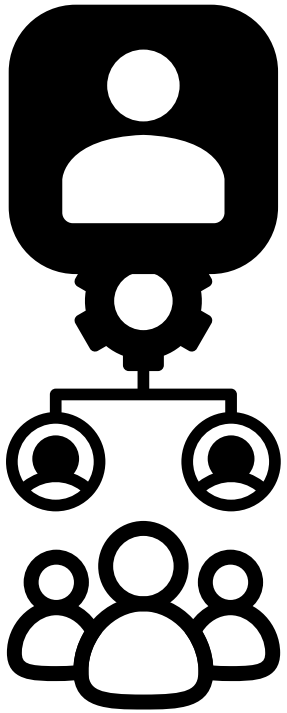
Tuebora
SELF DRIVEN IAM

How is policy-driven administration related with RBAC?

Access Control Policies

Accounts
Assigned Access

Permissions



Profiles
Lists of allowed access

Roles
Lists of accounts with allowed access

Groups
Lists of accounts

Tuebora
SELF DRIVEN IAM

Entitlements and Teams

Entitlements

- Roles that bundle together cohesive sets of permissions
- Business-friendly abstraction for requests and reviews
- Belong to applications
- Focal point for policy-driven administration
- Policies should reference teams whenever possible

Teams

- Roles that group sets of identities that share a certain characteristic
- Business-friendly abstraction for attribute values
- Organized by shared dimensions (shared characteristics)
- Referenced by entitlements for policies
- Policies usually reference identity attributes

Tuebora
SELF DRIVEN IAM

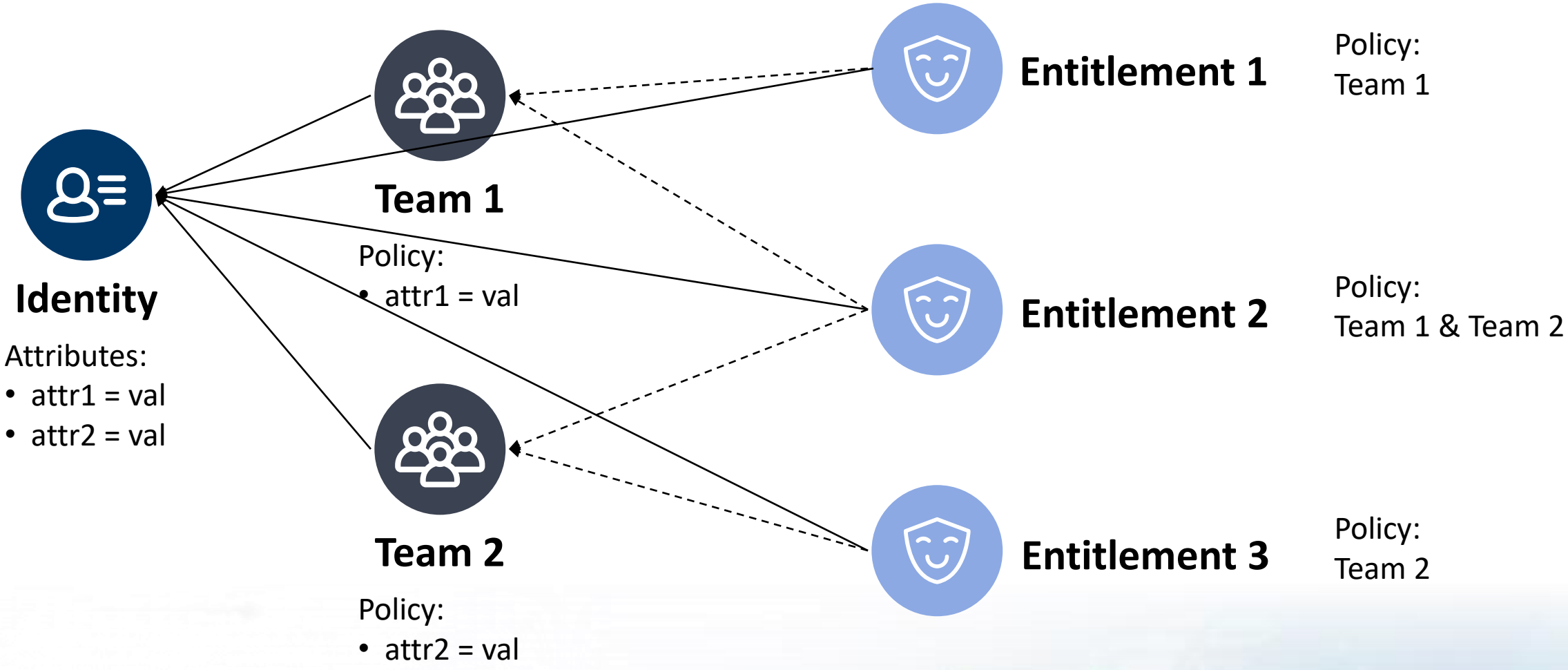
Context-aware IGA

Permission catalog

Entitlement catalog

Tuebora
SELF DRIVEN IAM

Roles make better attributes than attributes themselves



Tuebora
SELF DRIVEN IAM

Optimizing entitlements and policies

↑ Leverage

↓ Volatility

↓ Ceremony

+ Governance

Tuebora
SELF DRIVEN IAM

Entitlement/Policy Governance

Application owners exist and care deeply about their access risks

The Role of Artificial Intelligence

- **Tired:** Recommend entitlements to request or remove, approve/deny (in approvals) or accept/reject (in certification tasks)

- **Wired:** Recommend entitlements for assembly

- **Inspired:** Recommend policies for automatic assignment and removal of entitlements

Tuebora
SELF DRIVEN IAM

Policy-driven administration maturity

Maturity	Characteristics
Level 0	• No concept of identity • Possibilities are extremely limited
Level 1	• Identity foundation exists • Simple roles for bundling permissions, poor business-friendly abstractions • Possibilities remain limited, difficult to maintain
Level 2	• Entitlement catalog compresses permissions into business-friendly abstractions • Applications organize entitlements and provide governance structure • Policies are anchored to entitlements and attribute-driven
Level 3	• Abstractions for teams, entitlements and applications are fully realized • Policies, entitlements and teams are guided according to LVC+g model

Tuebora
SELF DRIVEN IAM

Recommendations

- ✓ Start with most critical applications
- ✓ Compress the administrative surface area with entitlements
- ✓ Track metrics to ensure overall objectives are being met
- ✓ Pay attention to leverage, volatility, ceremony and governance when modeling entitlements and policies
- ✓ Onboard more applications and repeat

Tuebora
SELF DRIVEN IAM