Document History

Date	Comment	Contributor
2023-06-16	Initial framework document	A. Hughes
2023-06-24	Additional content in the prior art and related work	D. Brossard
2023-06-27	Added related work: NGAC	A. Babeanu
2023-06-27	Added reference to Zanzibar systems and paper	O. Gazitt
Jul 27, 2023	Restated the purpose and used the alternate suggested name. Also added the AuthZAPI as a proposed deliverable	Atul Tulshibagwale
August 4, 2023	Added in OAuth2 & OIDC as additional potential target protocol for this	Mark Haine
August 15, 2023	Group call discussing the document - several updates	Group
August 22, 2023	Group call discussing the document - updates to scope and anticipated contributions	Group
September 12	Group call to finalize document prior to submission to Specifications Council	Group
September 29	Edits based on Specifications Committee feedback	Gerry Gebel

1) Working Group Name

Authorization Exchange WG (AuthZEN WG)

2) Purpose

The purpose of the AuthZEN WG is to provide standard mechanisms, protocols and formats to communicate authorization related information between components within one organization or across organizations, which may have been developed or sourced from different entities.
Centralized authentication services have revolutionized identity management and security best practices by removing the burden of repeatedly implementing identity lifecycle management within individual applications and by giving users a more seamless and consistent authentication experience. Protocols such as SAML and OIDC facilitate this approach to single sign-on and federated environments.

Authorization capabilities are in need of a similar paradigm shift to enable applications to better support more fine-grained, dynamic authorization than what is afforded by today's commonly used pattern of embedding entitlements into OAuth2 bearer tokens after user authentication. This is not a new idea and we already have various approaches to implementing externalized authorization – commonly called "P*P" architectures (PIP, PDP, PEP, etc.). Examples include architectures based on IDQL, OPA/Rego, XACML and Zanzibar. Deploying any of these authorization architectures can be challenging from implementation complexity, granularity, and scalability perspectives; interoperability between different architectures and between different implementations are particularly challenging.

The purpose of this WG is to explore how to improve the deployability, scalability and interoperability of dynamic, fine-grained authorization schemes to better meet the needs of modern information security best practices. In particular, we need to make authorization easy for an organization to deploy and operate authorization capabilities across their entire application estate, including both SaaS services and internally developed applications (whether they be on-prem or in the Cloud).

Note that this is not necessarily an effort to define yet another authorization architecture or runtime policy language. Instead, the WG will develop OpenID Foundation Final Specifications which leverage existing architectures and protocols as much as possible. Where appropriate , the WG intends to collaborate with international standards development organizations, such as ISO/IEC JTC 1, ITU-T, and IETF, for recognition of these OpenID Foundation specifications.

3) Scope & Objectives

“Be the OAuth2/OIDC/SAML of authZ” by:

1) Increase interoperability between existing standards and approaches to authorization - examples include ALFA, Cedar, OPA, IDQL, Graph-based and Zanzibar-inspired systems such as OpenFGA, Topaz, SpiceDB.
    a) interop from a policy management perspective
2) Define and formalize interoperable communication patterns between major authZ components, for example PAP, PDP, PEP, and PIP.
    a) use cases
    b) integration patterns
    c) interop from a runtime request/response perspective
3) Establish and promote the use of externalized authZ as the preferred pattern.
    a) Single pane of glass for management and auditability for those who manage application portfolios.
    b) Software developers/owners/SaaS are relieved of this burden and don’t have to reinvent the “authorization wheel” by making authZ a utility so that it is easy to plug into an application
    c) Compliance requirements are more easily and cost-effectively met with provable controls that foster more transparency

Out of scope

- Providing higher abstraction level of technical policies for an executive audience

4) Proposed specifications

1. Description of standard authorization patterns, use cases, communications patterns, and integration patterns.
2. An API to communicate authorization requests and decisions between Policy Decision Points (PDPs) and Policy Enforcement Points (PEPs) (which may be implemented by different parties).
3. An API to communicate authorization policy and data from PAP to PDPs (which are implemented by different parties).

5) Anticipated audience or users

- Authorization developers and architects
- SaaS vendors (Multi client hosting)
- Cloud platforms
- Application vendors
- Enterprise implementers/practitioners who integrate authorization products.

6) Language

English.

7) Method of work

E-mail discussions on the working group mailing list, working group conference calls, and face-to-face meetings from time to time.

8) Basis for determining when the work is completed

When 3 independently-developed implementations that are proven to interoperate exist!

9) Related works

- OASIS XACML: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml
- XACML ALFA: https://en.wikipedia.org/wiki/ALFA_(XACML)
- NIST ABAC: Guide to Attribute Based Access Control (ABAC) Definition and Considerations: NiST SP 800-162
- ANSI / NIST Next Generation Access Control (NGAC): INCITS 565-2020
- Google Zanzibar: https://research.google/pubs/pub48190/

- OpenID Connect Advanced Syntax for Claims: https://openid.bitbucket.io/ekyc/openid-connect-advanced-syntax-for-claims.html
- RFC 3198 Terminology for Policy-Based Management https://www.rfc-editor.org/rfc/rfc3198
- RFC 2753 A Framework for Policy-based Admission Control https://www.rfc-editor.org/rfc/rfc2753
- RFC 2904 AAA Authorization Framework https://www.rfc-editor.org/rfc/rfc290410)
- IDQL/Hexa project Hexaorchestration.org https://github.com/hexa-org
- Open Policy Agent: https://openpolicyagent.org

Anticipated contributions

Authorization Design Patterns:

[Policy-Charter] Authorization Design Patterns

Proposed standard for PEP to PDP authorization API:

https://sgnl-ai.github.io/authzapi/

10) Proposers

- Atul Tulshibagwale, SGNL, atul@sgnl.ai
- Gerry Gebel, Strata Identity, gerry@strata.io
- Steve Venema, ForgeRock, steve.venema@forgerock.com
- Omri Gazitt, Aserto, omri@aserto.com
- Pieter Kasselman, Microsoft, pieter.kasselman@microsoft.com
- Alex Babeneau, 3Edges, alex@3edges.com

- David Brossard, Axiomatics, david.brossard@axiomatics.com
- Allan Foster, allan@macguru.com
- Andrew Hughes, Ping Identity, andrewhughes@pingidentity.com
- Mike Kiser, SailPoint, mike.kiser@sailpoint.com