

ALFA 2.0

the Abbreviated Language for Authorization

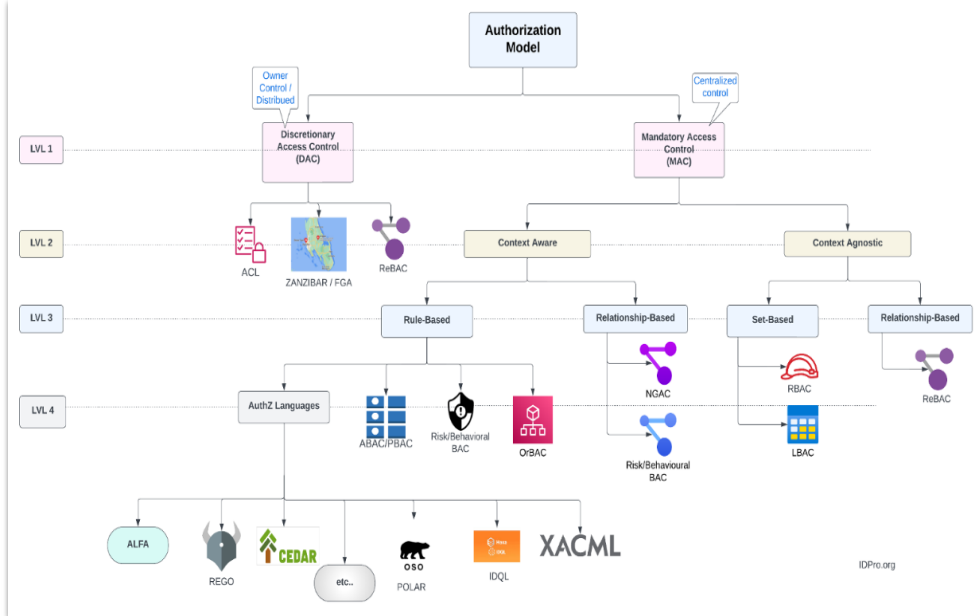
Theo Dimitrakos

t.dimitrakos@kent.ac.uk

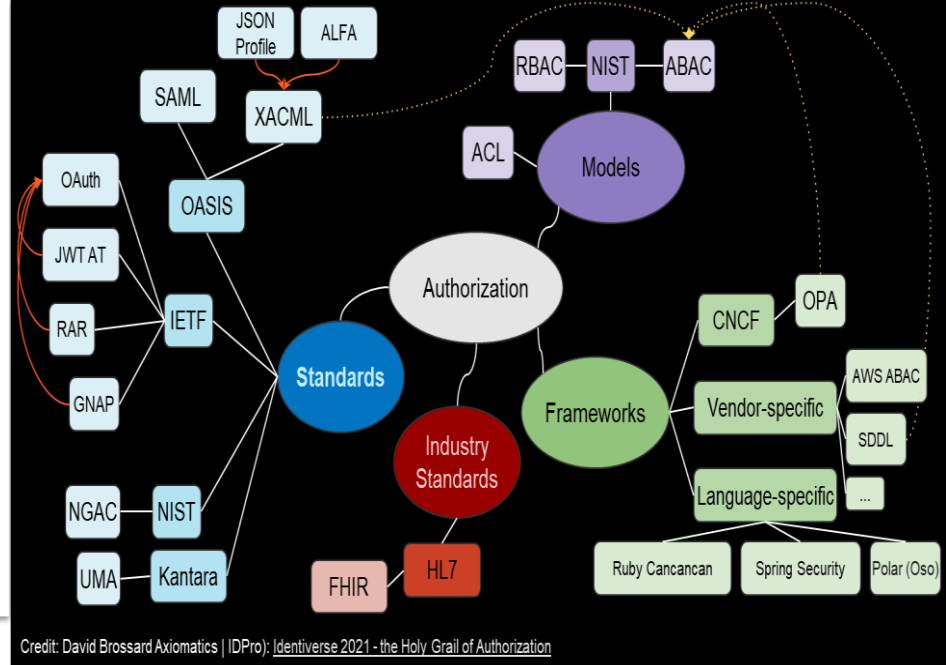
theo.dimitrakos@huawei.com

theo.dimitrakos@ifiptm.org

Based on presentation at IETF120 by
David Brossard
CTO, Axiomatics

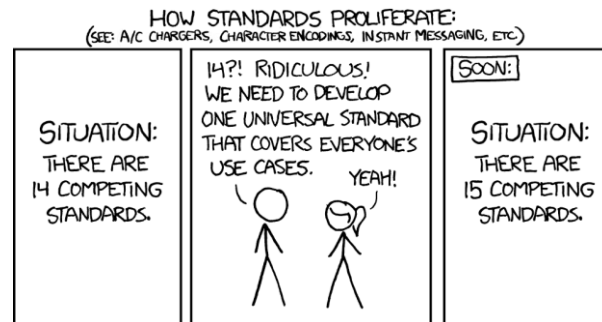
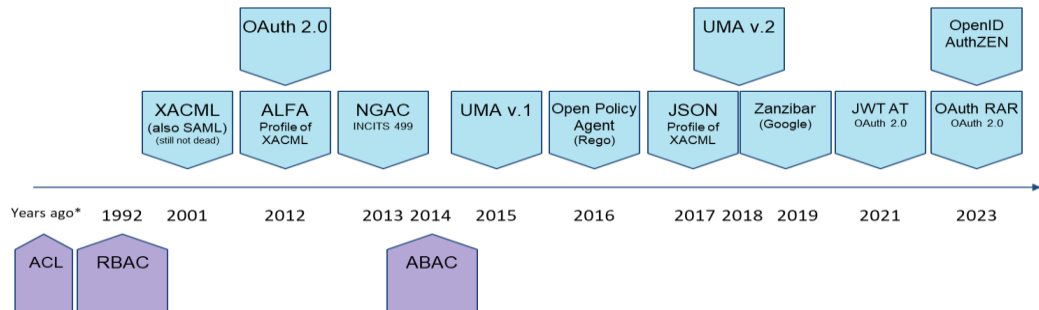


Credit: Alex Babeanu (3Edges | IDPro): <https://idpro.org/a-taxonomy-of-modern-authorization-models/>



Credit: David Brossard Axiomatics | IDPro: [Identiverse 2021 - the Holy Grail of Authorization](https://idpro.org/a-taxonomy-of-modern-authorization-models/)

Standards, Frameworks & Models Timeline



Source: [xkcd Standards](https://xkcd.com/142/)

What is ALFA

- Abbreviated Language for Authorization
- Implements RBAC, ABAC, ReBAC in one single language
- Drafted under OASIS XACML in March 2014
- Aimed at developers
- All the goodness of XACML, (almost) none of the bad
- Strong uptake within XACML implementations

Who is interested in ALFA 2.0?



Note: This slide is not an endorsement of ALFA by the parties mentioned

Why ALFA 2.0?



*Get rid of the XACML
Baggage*



*Strong need for
standardized AuthZ*



Promote reuse



*Avoid Cloud platform
proprietary options*



Simplify ALFA

Who uses ALFA today?

Thales developed the AuthZForce XACML 3.0 PDP as part of Fiware and released via an Open Source initiative called [OW2](#). [FIWARE](#) is an open source cloud platform.

ALFA is called out in [official documentation](#).

Rock Solid Knowledge have been using ALFA for 5+ years. They have a native C# PDP that uses ALFA which is then “compiled to native”. Their PDP is part of their IAM suite

Customers use it to write their policies



AXIOMATICS



Salesforce uses XACML internally and ALFA to help write policies.

THALES



HUAWEI

Huawei R&D have been using ALFA for 5+years. They have a native C/C++ PDP that uses ALFA natively to evaluate policies, and a Usage Control (UCON) extension in the form of an ALFA profile that is used as a C/C++ library or via a GoLang service wrapper in various product prototypes including devices, cloud, dataspace connectors



Rock Solid Knowledge

Why ALFA at IETF?

Theo's perspective

0.2 – 0.8 (<1 millisecond on Linux & i7)

Good for humans

- Simple but expressive
- Clear and intuitive for humans to understand
- Nice target for C-NLP interface

Good for machines

- Enforceable policies
 - First two native evaluators + new FOSS planned
 - Numerous via XACML interpretation
- Attribute based
- Supports obligations (actions) enforcement linked to decisions
- Policy combination algorithms provide a simple way of resolving conflicts when they appear

Internet Scale

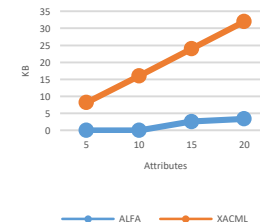
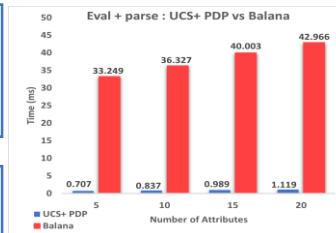
- **Small**: small computational print, ultra-efficient
- **Big**: service ready with API & enforcement protocols
- **CC**: ready for compute continuum: examples of specializations in IoT device, edge, cloud, network C&O, dataspace
- Supports **decentralized multi-administration** scenarios

Rigorous

- Leverages ABAC and XACML experience
- Formal semantics & formal analysis tools: static (ASP) and dynamic (RTLola)

Extensible

- Reuse of various XACML profiles for verticals
- Tested as an excellent foundation for executing data/resource usage control
- Trust management policy profile



ACM SACMAT 2024
<https://dl.acm.org/doi/10.1145/3649158.3657038>

ACM SACMAT 2023
<https://dl.acm.org/doi/10.1145/3589608.3593843>



<https://www.springerprofessional.de/en/collaborative-approaches-for-cyber-security-in-cyber-physical-systems/23882556>



Next Steps

Questions

- Should ALFA 2.0 be its own WG?
- Should it be part of OAuth? Other WG?

Useful links

- [ALFA 2.0 - the Abbreviated Language for Authorization](#) - draft RFC submission
- ALFA reference site: <https://alfa.guide>
- [ALFA Slack Community](#)
- <https://github.com/davidjbrossard/alfa-authorization-language>

Thank you