

Open Standards for the Intelligent Trust Fabric

ALEX SIMONS

Corporate Vice President · Product Management
Microsoft Identity & Network Access



Identity
Geeks



Volleyball
Geeks



Identity
Geeks



Volleyball
Geeks

Trust Fabric

Identity infused everywhere

- Trustworthy
- Built in privacy and control
- Multi-Cloud, Multi-Device
- Self-securing
- Based on open standards



Another Amazing Year in Identity Standards

Policy/Regulatory Guidance



SP 800-63-4: Digital Identity Guidelines

Draft.



Identity & Access Management Roadmap

Draft.



EUDI Wallet Architecture & Reference Framework 1.0.0

Draft

Access



I E T F

OAuth Demonstrating Proof-of-Possession

Awaiting final publication.



I E T F

Cross-device Flows: Security Best Current Practices

Draft 01.



Shared Signal Framework RISC Profile

Progressed to 2nd implementers draft.

Automation



I E T F

SCIM Use Cases & Concepts

Initial draft.



I E T F

Cursor-based Pagination of SCIM Resources

Initial draft.



I E T F

SCIM Roles and Entitlements

Initial draft.

Another Amazing Year in Identity Standards

Decentralization & Direct Presentation



OpenID4VC Specifications Family

Presentation: 2nd implementers draft.

Issuance: 1st implementers draft.

Presentation over BLE: WG draft.

SIOP v2: 1st implementer's draft.



Selective Disclosure for JWTs (SD-JWT)

Draft 04.



Verifiable Credentials Data Model

Work is under way.



JWT VC Presentation Profile

Draft.



ISO 18013-7 - Personal identification — ISO-compliant driving license — Part 7: Mobile driving license (mDL) add-on functions

Work is under way.



ISO 23220 mobile eID Documents

Work is under way.

Authentication



Client-to-Authenticator Protocol 2.2

Draft 1 in public review.



WebAuthn L3

Work is under way.



OAuth Step-up Authentication

Awaiting final publication.



ISO 27553-1 Security and privacy requirements for authentication using biometrics on mobile devices — Part 1: Local modes

Final

Key Standards Initiatives

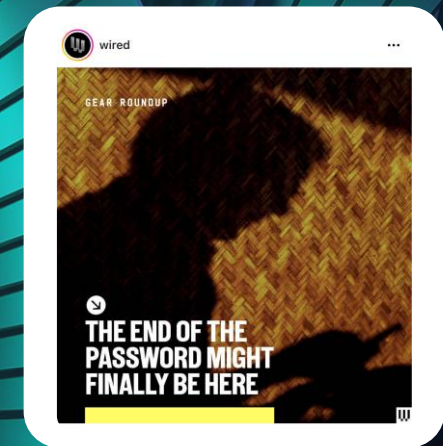
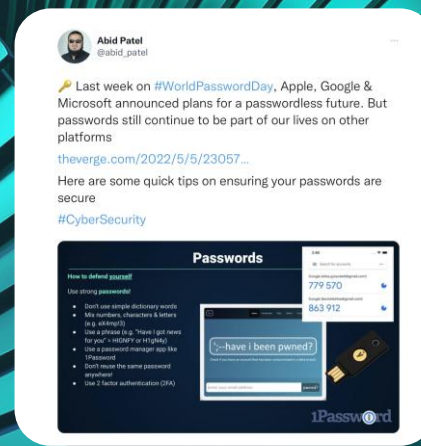
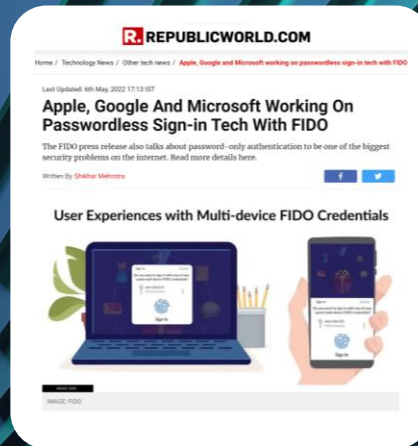
- Strong Authentication
- Decentralized Identities
- Machine Identities
- Authorization Policy

Key Standards Initiatives

- Strong Authentication
- Decentralized Identities
- Machine Identities
- Authorization Policy

One year ago...
PASSKEYS

CONGRATS
on passkeys



 **identiverse® 2022**

#identiverse

Today, going mainstream...

PASSKEYS

tom's guide


Home Best Picks News Reviews How Tos

Kill passwords forever — here's how to set up passkeys on iPhone, iPad and Mac

By David Crookes last updated December 09, 2022

It's time to ditch passwords and learn how to set up passkeys on iPhone, iPad and Mac instead

f t i y p r m Comments (0)



(Image credit: Tom's Guide)

40 YEARS PC

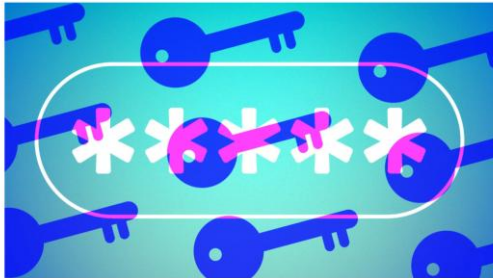
Home > How-To > Security > Password Managers

How to Set Up Passkeys for Your Google Account

Passkeys are easier to use and more secure than passwords, but getting started with them isn't simple. We tell you how to set up and use passkeys for Google on all your devices.

By Max Eddy
May 15, 2023

f t ...



(Credit: René Ramos)

techradar

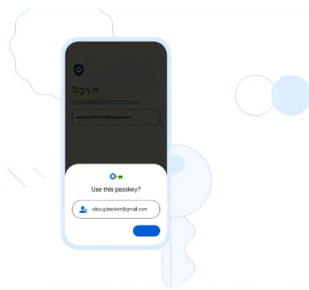
Home > How-to > Software

Passwords are dead: how to set up a passkey for your Google or Gmail account

By Cesar Cadenas published 15 days ago


A more convenient way to protect your information

f t i y p r m



(Image: © Google)

THE WALL STREET JOURNAL.



PERSONAL TECHNOLOGY: NICOLE NGUYEN

Hate Passwords? It's Time to Try Passkeys

A new type of login is easier and safer to use than passwords—with caveats



DEMO



ROBIN GOLDSTEIN

Partner Director · Product Management
Identity & Network Access



PASSKEYS: What's next



Enhancing the password to passkey transition experience for users



Improving the manageability of passkeys for end users



Balancing great user experiences with high assurance security requirements

Key Standards Initiatives



Strong Authentication



Decentralized Identities

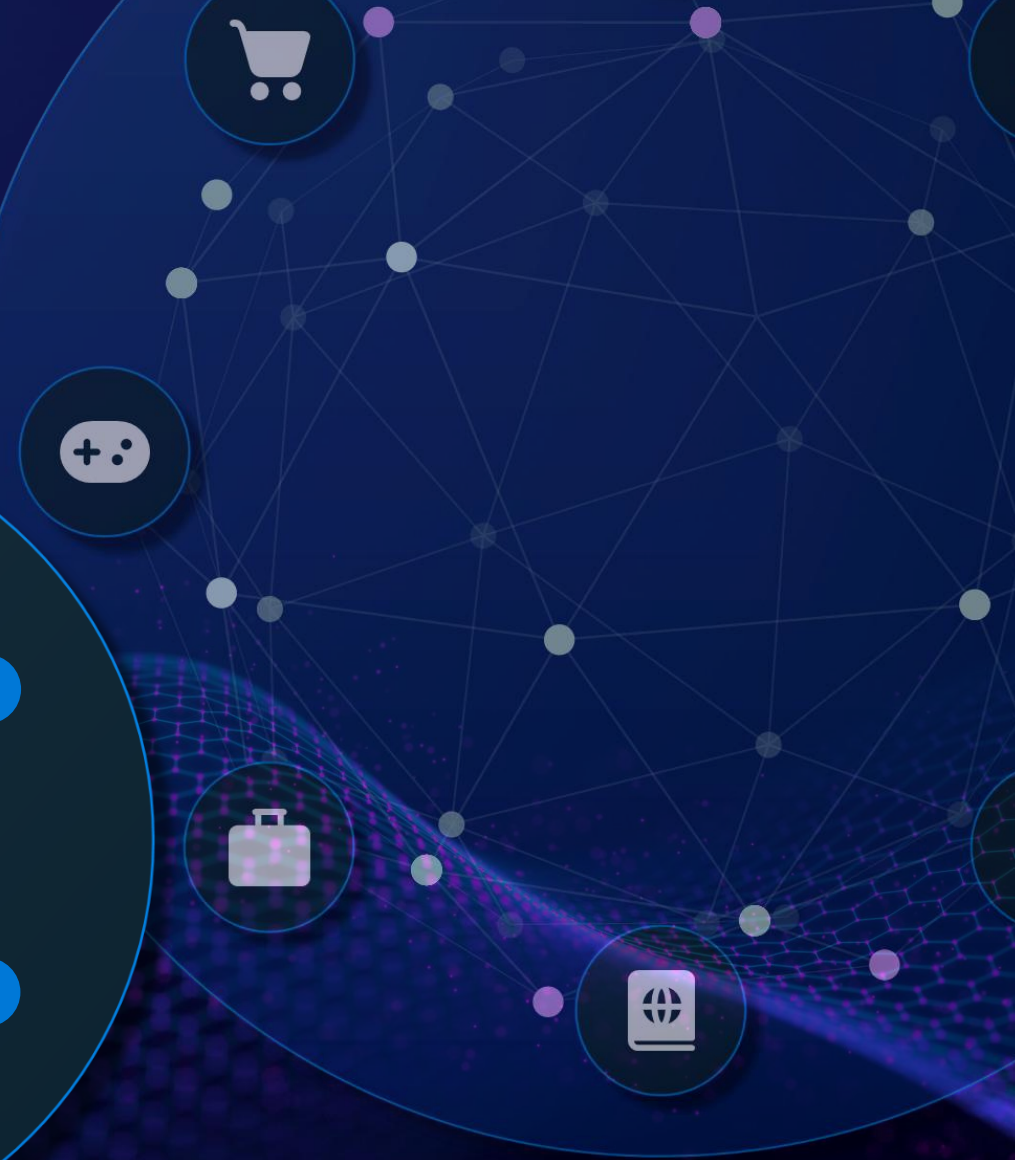


Machine Identities



Authorization Policy

Momentum is building:
**DECENTRALIZED
IDENTITIES**



EUDI Wallet Use Cases



Identification and
authentication to
access online services



Mobility and
digital driving
license



Health



Educational credentials
and professional
qualifications



Digital Finance

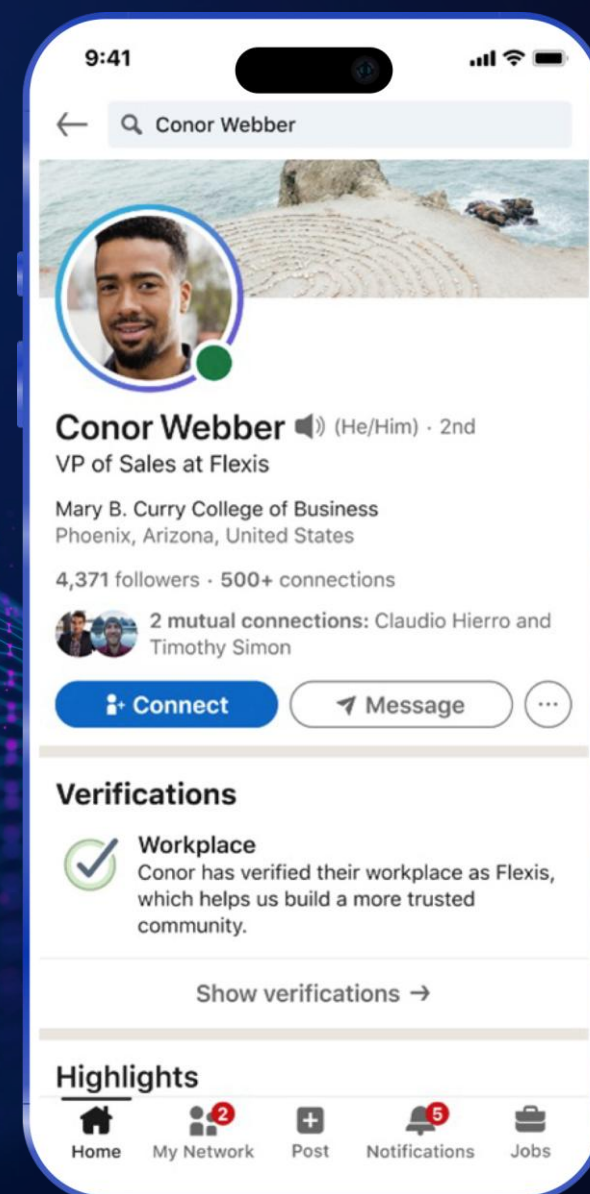
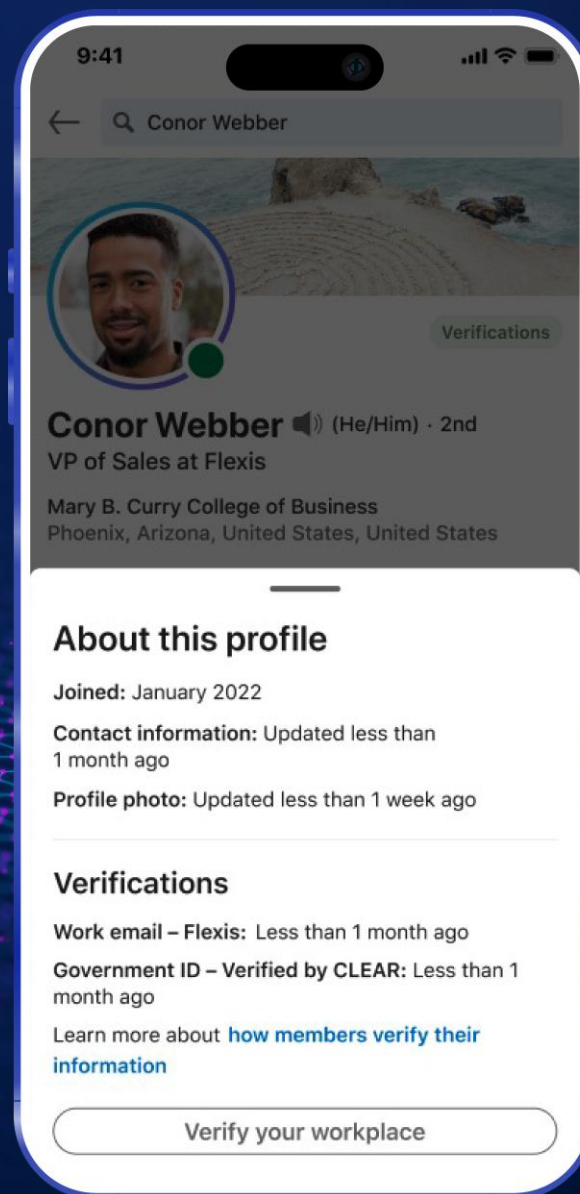


Digital Travel
Credential



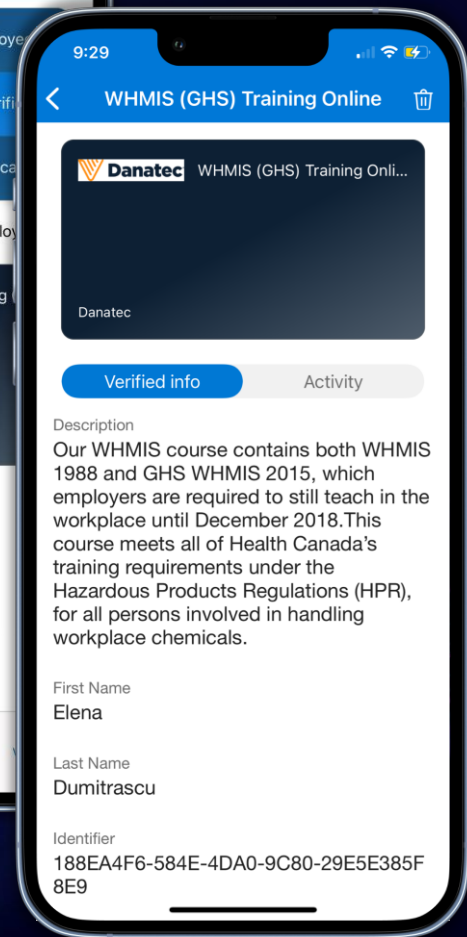
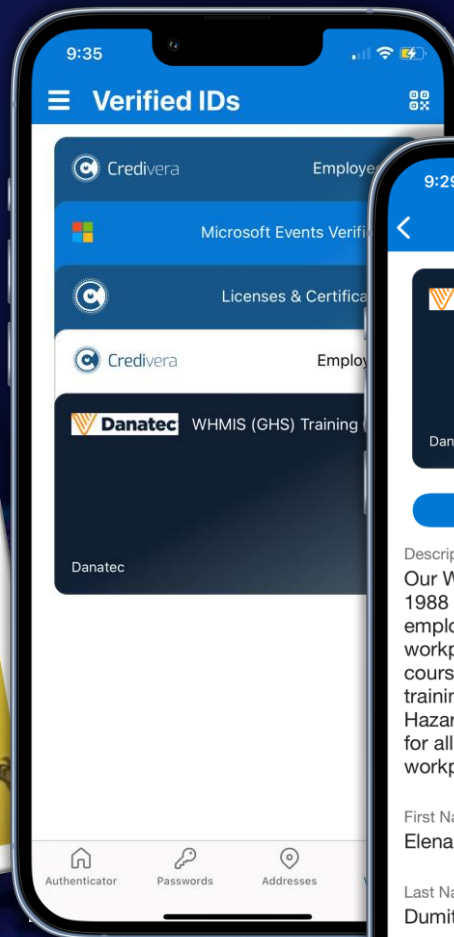
Decentralized Identities real world deployments

- Real people
- Real credentials
- Real jobs





CANA
CONSTRUCTION



#identiverse



VIDEO

Decentralized identity real-world deployments



Credivera



#identiverse



Next big challenge:
GOVERNMENT-ISSUED IDENTIFICATION



Key Standards Initiatives



Strong Authentication



Decentralized Identities



Machine Identities



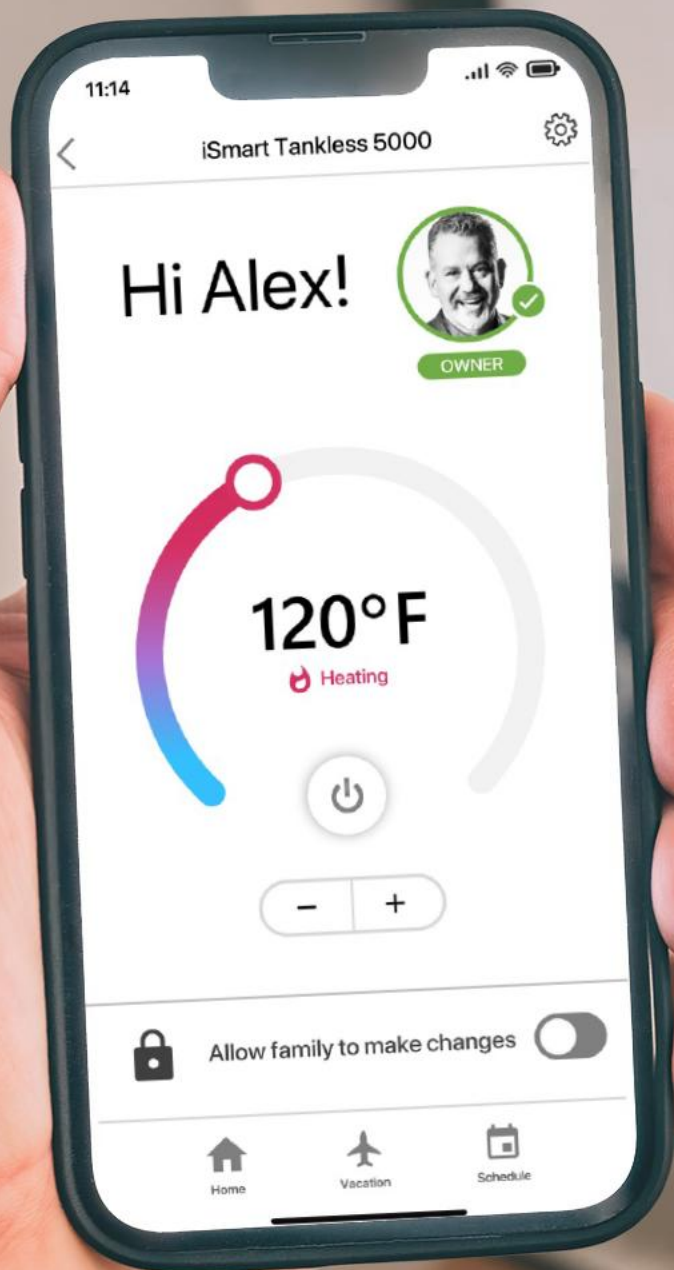
Authorization Policy

MACHINE IDENTITIES



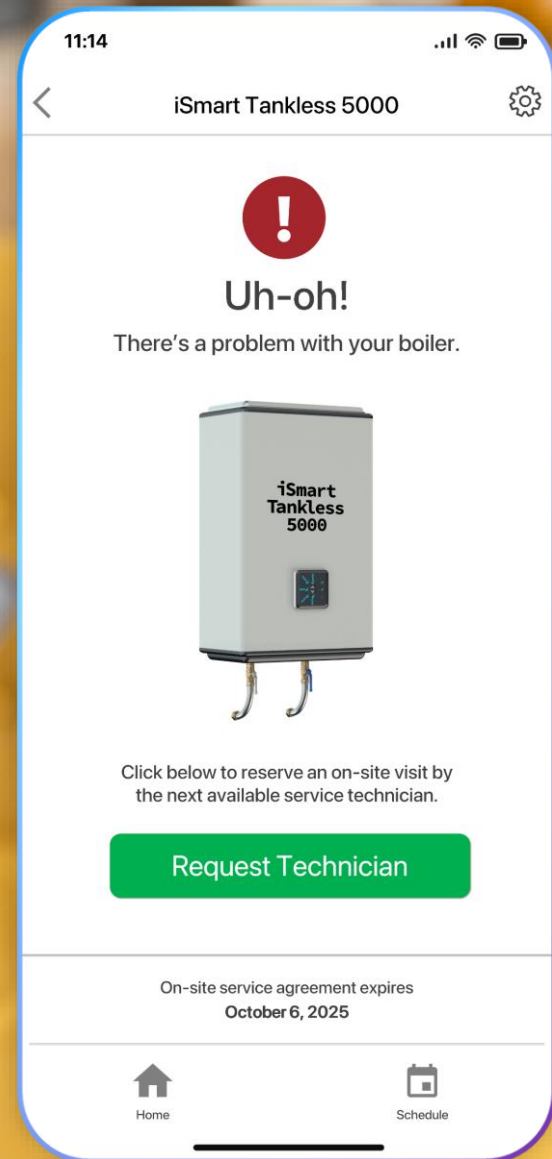
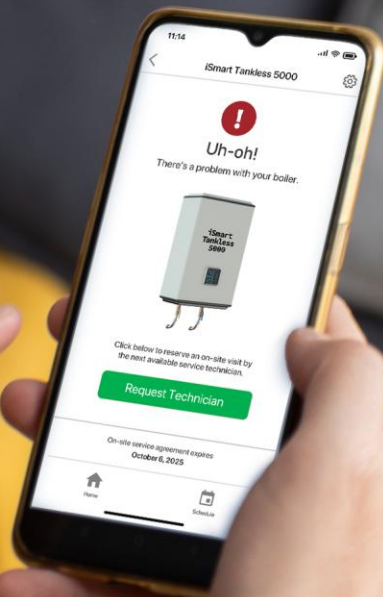
**iSmart
Tankless
5000**





iSmart
Tankless
5000







Customer

Alex Simons
123 Main Street
Redmond, WA 98055



Service Request

June 2, 9:00 AM

TICKET NUMBER: 1078496
MODEL: Smart Tankless S1000
ERROR CODE: 6231n43M4w398t



Mark Johnson
Certified Smart Technician
Certified Smart Diagnostician

Scan to verify
credential and allow
access.





**EVAN
GILMAN**

Maintainer:  spiffe  SPIRE

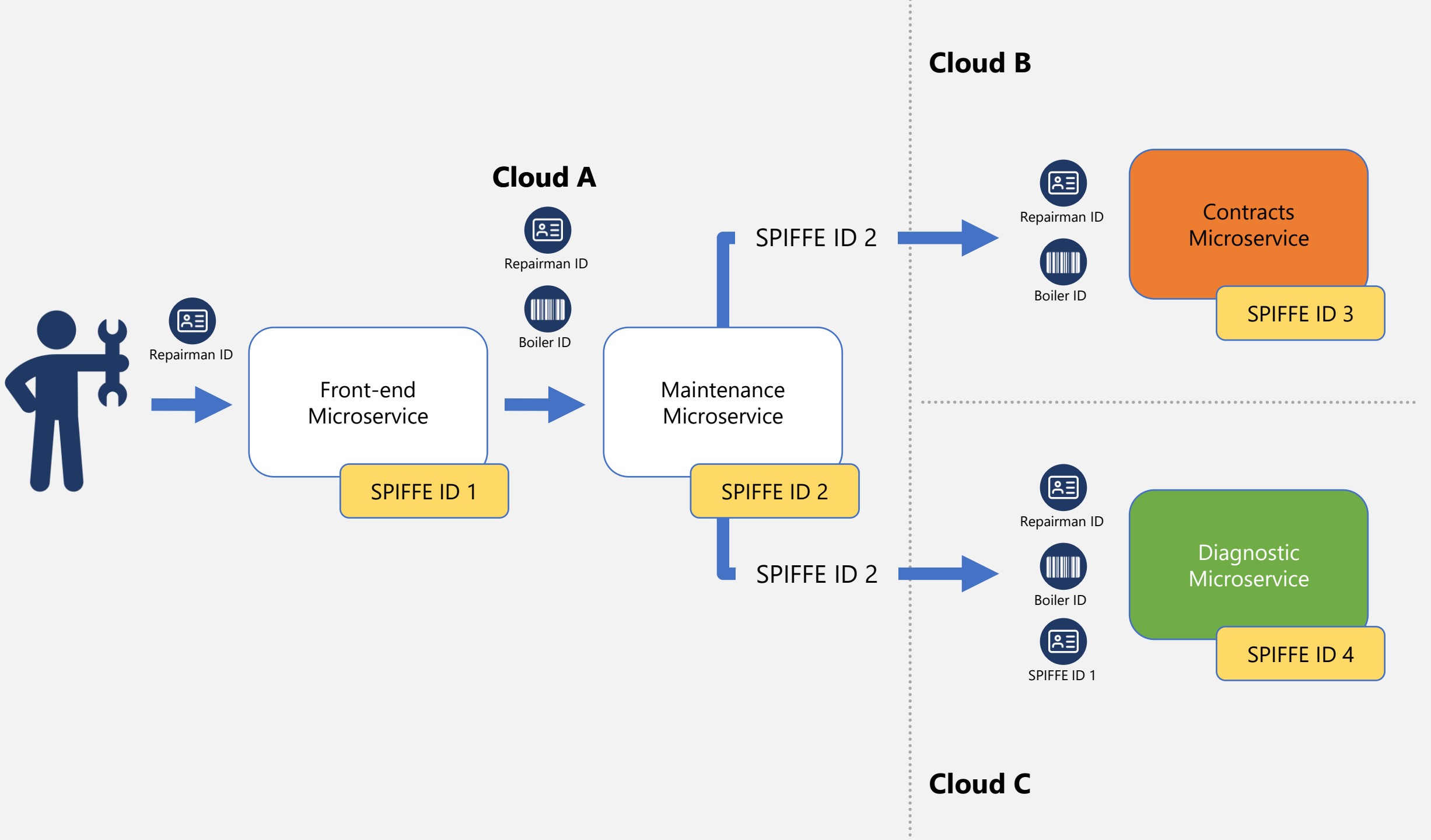
Co-founder:  SPIRL

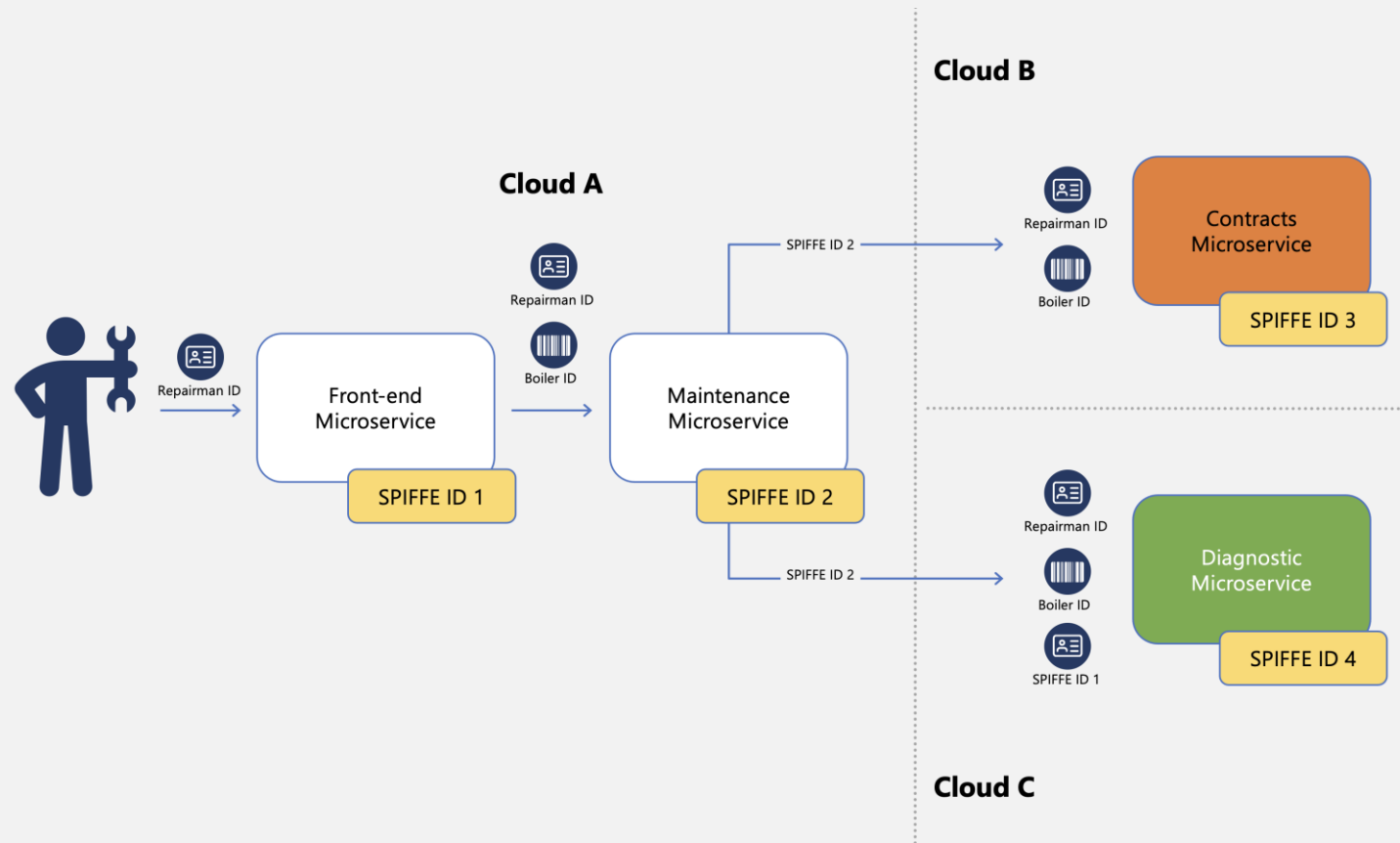


**PIETER
KASSELMAN**

Identity Standards Architect

 Microsoft





Making this real

We need standards for:



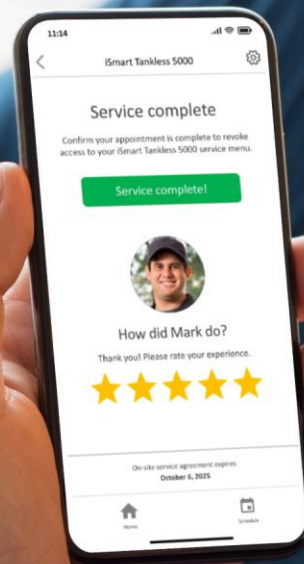
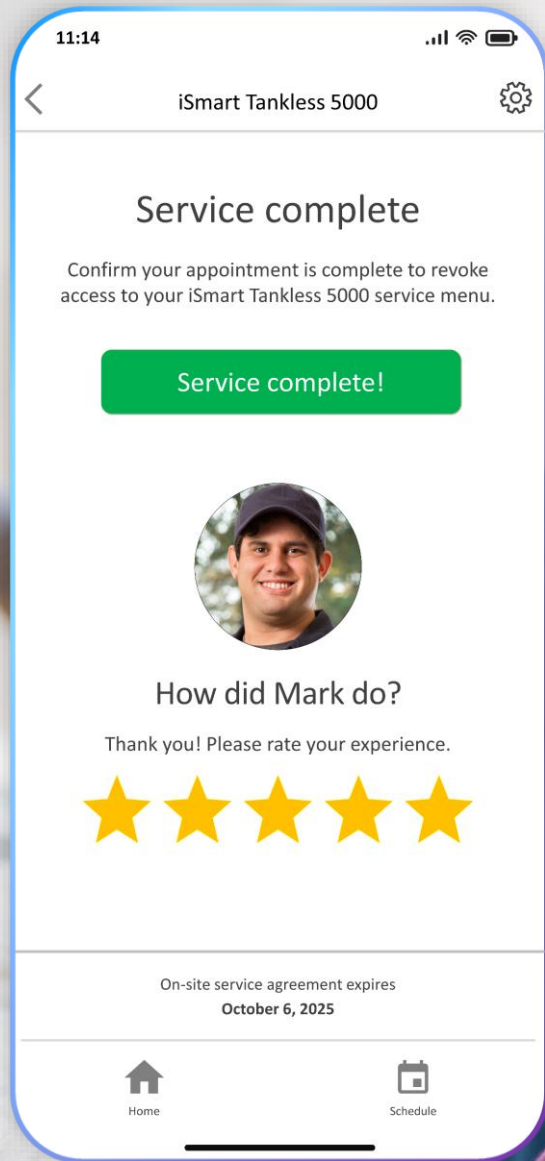
Preserving identity throughout the stack



Policy management



Fine-grained authorization



ALEX - ACCESS DENIED



Zone
□
□
□



Key Standards Initiatives



Strong Authentication



Decentralized Identities



Machine Identities



Authorization Policy



ZANZIBAR

Idol

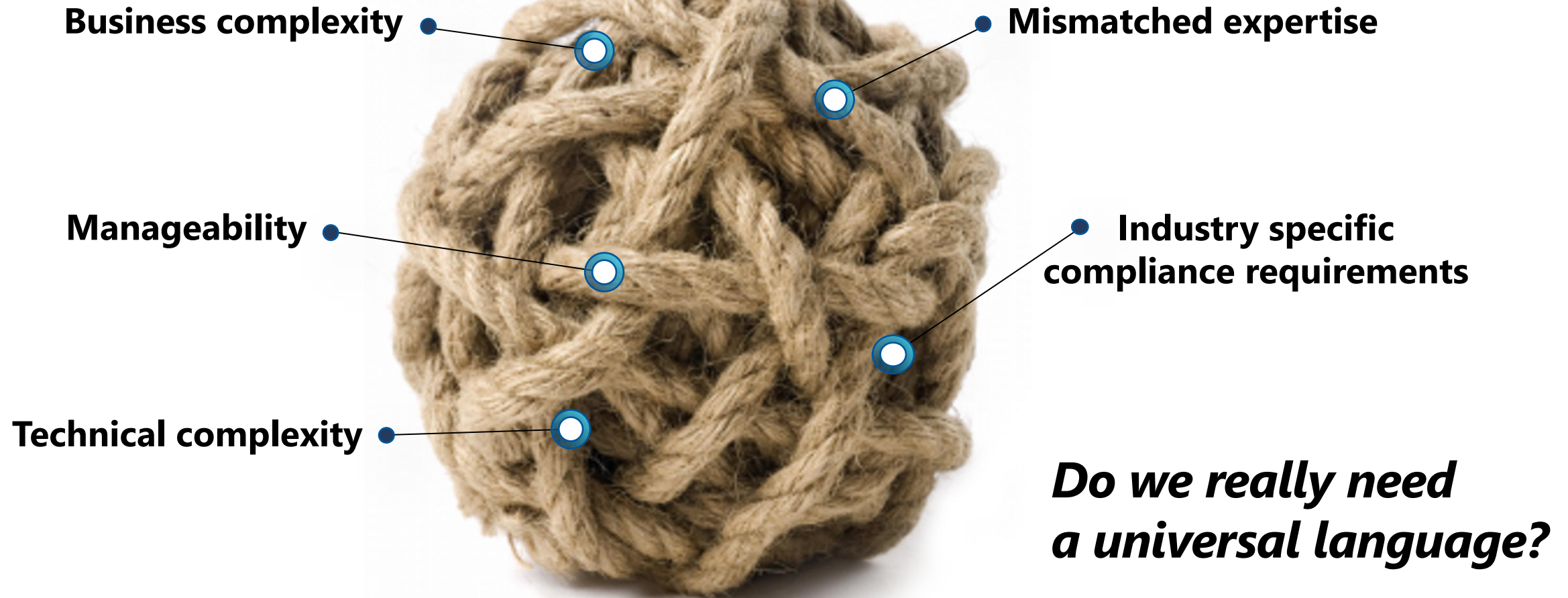
NGAC

OPA/Rego

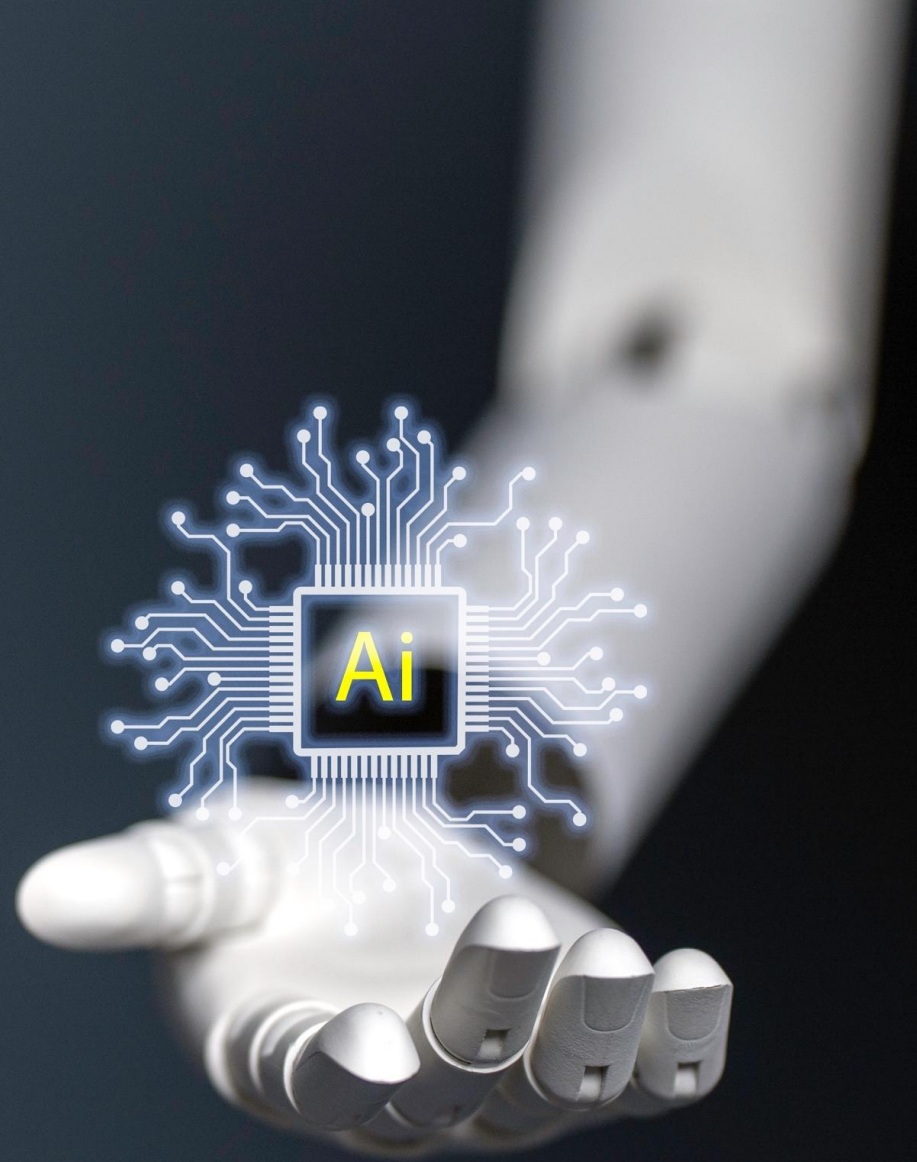
CEDAR

XACML

Why is this so hard?



**CAN AI HELP TO CUT
THE GORDIAN KNOT
OF AUTHORIZATION?**

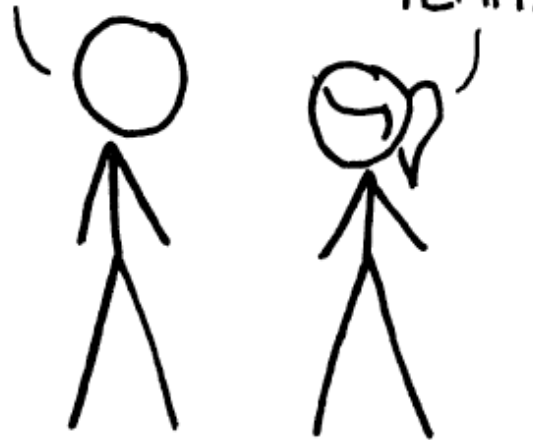


HOW STANDARDS PROLIFERATE:

(SEE: A/C CHARGERS, CHARACTER ENCODINGS, INSTANT MESSAGING, ETC.)

SITUATION:
THERE ARE
14 COMPETING
STANDARDS.

14?! RIDICULOUS!
WE NEED TO DEVELOP
ONE UNIVERSAL STANDARD
THAT COVERS EVERYONE'S
USE CASES.



SOON:

SITUATION:
THERE ARE
15 COMPETING
STANDARDS.

Microsoft Security Copilot

Preview

/

My investigations


/

Please create a policy that allows a boiler owner to set the temperature and tim...

DAILY TIP

Your goals are Copilot's goals

Tell it what you want it to do. If Copilot gets it wrong at first, redirect it by editing the prompt, adding more info as needed.



Export

Please create a policy that allows a boiler owner to set the temperature and timer for their boiler. Express these policies in Rego, Azure RBAC, and Cedar.

Summary

Pinned Items (0)

Pin responses to summarize evidence for your investigation

Prompt | Determining most relevant skill

Prompt | No skill matched

Prompt | Composing final output

Prompt | Done

Here are the policies expressed in Rego, Azure RBAC, and Cedar for allowing a boiler owner to set the temperature and timer:

Rego (Open Policy Agent):

```
package boiler

default allow = false

# Allow boiler owner to set temperature and timer
allow {
    input.user.role == "boilerOwner"
    input.action == "setTemperature"
}

allow {
    input.user.role == "boilerOwner"
    input.action == "setTimer"
}
```

Azure RBAC (Role-Based Access Control):

1. Create a custom role definition for the boiler owner:

```
{
  "Name": "Boiler Owner",
  "IsCustom": true,
  "Description": "Allows a boiler owner to set the temperature and timer",
  "Actions": [
    "Microsoft.Boiler/setTemperature/action",
    "Microsoft.Boiler/setTimer/action"
  ],
  "AssignableScopes": [
    "/subscriptions/{subscriptionId}",
    "/subscriptions/{subscriptionId}"
  ]
}
```

2. Assign the custom role to the boiler owner.

Cedar (Configuration Language for Authorization):

```
...

@id("boiler-owner-policy")
permit(
    principal == User::"boilerOwner",
    action in [Action::"setTemperature", Action::"setTimer"],
    resource == Boiler::"boilerID"
);
...
```

These policies should help you achieve the desired access control for the boiler owner.

Confirm

Off-target

Report

Pin

Tell me what this policy does and then translate the policy to Cedar:

```
package boiler.maintenance
default allow = false
allow {
    input.agent.role == "maintenance"
    input.agent.qualification == "qualified"
    input.contract.status == "active"
    valid_action
}
valid_action {
    action := input.action
    action == "run diagnostics"
}
valid_action {
    action := input.action
    action == "change settings"
}
valid_action {
    action := input.action
    action == "update firmware"
}
```

Prompt | Determining most relevant skill

Prompt | Matched low-level skill (based on description): FunctionName: GenerateSecurityExamples Inputs: GenerationInstructions: "Translate the policy expressed in Rego into a policy expressed in Cedar"

Prompt | Skill 'GenerateSecurityExamples' completed

Prompt | Composing final output

Prompt | Done

The policy you've posted appears to be written in the Open Policy Agent (OPA) language called Rego. OPA is a general-purpose policy engine that unifies policy enforcement across the stack and is often used in cloud-native environments.

The policy defines rules for allowing an agent (possibly a software service or user) to perform certain actions on a "boiler maintenance" package. Let's break it down:

• By default, all actions are denied ('**default allow = false**')
• An action is allowed ('allow') if the following conditions are met:

- The '**agent**' performing the action has a '**role**' of "maintenance" ('**input.agent.role == "maintenance"**').
- The '**agent**' performing the action has a 'qualification' of "qualified" ('**input.agent.qualification == "qualified"**').
- The '**contract**' for the maintenance is "active" ('**input.contract.status == "active"**').

- The action taken is deemed a '**valid_action**'.
- A '**valid_action**' is defined as either "run diagnostics", "change settings", or "update firmware".

To sum up, this policy allows a qualified maintenance agent to run diagnostics, change settings, or update firmware on a boiler system, but only if the maintenance contract is active.

Here's the translation of the boiler owner policy from Rego to Cedar:

Cedar Policy

```
...

@id("boiler_maintenance_policy")
permit(
    principal, // could be replaced with specific user id using UUID
    action in [Action::"run_diagnostics", Action::"change_settings", Action::"update_firmware"],
    resource == Resource::"boiler" // assuming "boiler" is the resource id
)
when {
    principal.role == "maintenance" &&
    principal.qualification == "qualified" &&
    resource.contract.status == "active"
};
...
```

In this translation, the Rego policy's rules and conditions are mapped to corresponding Cedar constructs. The Cedar policy achieves the same access control for the boiler owner as the Rego policy.

Confirm

Off-target

Report

Pin

Ask anything about security, or type / for suggestions

AI-generated content can have mistakes. Make sure it's accurate before using it.



Solving the puzzle with Large Language Models

Key Standards Initiatives



Strong Authentication



Decentralized Identities



Machine Identities



Authorization Policy

Trust Fabric

Identity infused everywhere

- Trustworthy
- Built in privacy and control
- Multi-Cloud, Multi-Device
- Self-securing
- Based on open standards



What's next?



Support and Adopt passkeys



Plan for how you'll use VCs and DIDs



Adopt Zero Trust Architectures for your workloads



THANK YOU!