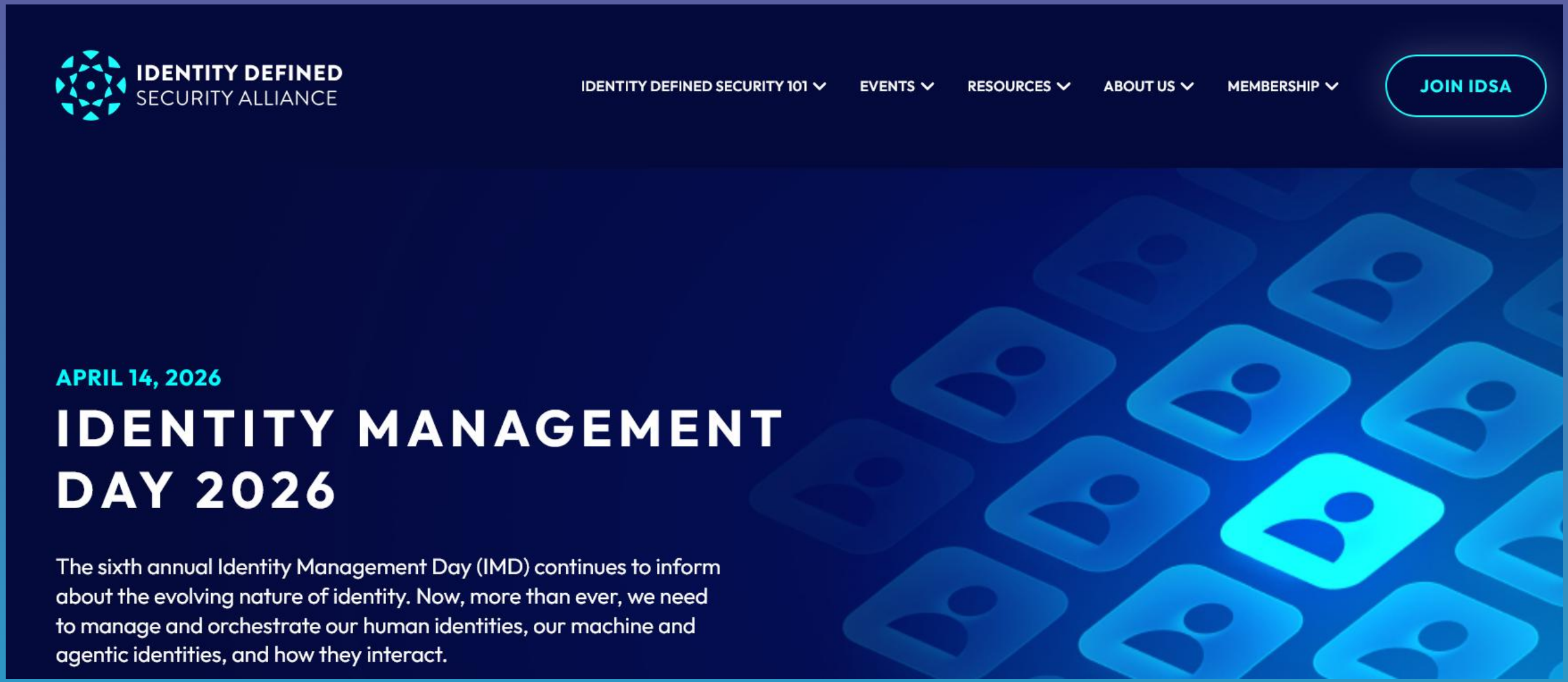
Platform voor InformatieBeveiliging

# Future State of Access

PvIB IAM kennisavond

14 april 2026



# André Koot

- Security & IAM Consultant
- Author/trainer IMF-academy
- Co-founder PvIB SIG IAM
- Member BoK Committee IDPRO
- Former editor (in chief) PvIB Informatiebeveiliging
- @meneer@social.myfed.space
- https://linkedin.com/meneer

**December 2020**
Founded in the Netherlands

**July 2022**
Founded the Regensburg office

**+ 25**
IAM Business Experts

**Vision:**
We help people, machines, and companies connect data in an intelligent and secure way to leverage the possibilities of digital ecosystems.

# This is sonicbee

Your strong partner for Identity and Access Management (IAM). We offer thoughtful and innovative consulting approaches. Our goal? To make companies smarter, faster, and safer.
Become a pioneer in identity and access management:

*“Who can access what and why?”*

**Let‘s Go!**

# Future state of access

- First: Rewind 20 years
- Then: Fast forward to today
- And: Further forward to the future

## 20 years ago I wrote:

# ‘RBAC is EOL’

- Roles are local
- Governance issues
  - What authz are in a role and who decides?
  - Who gets a role and who decides?
  - How about nested groups?
- Roles have no context
- Roles are static

## 20 years ago…

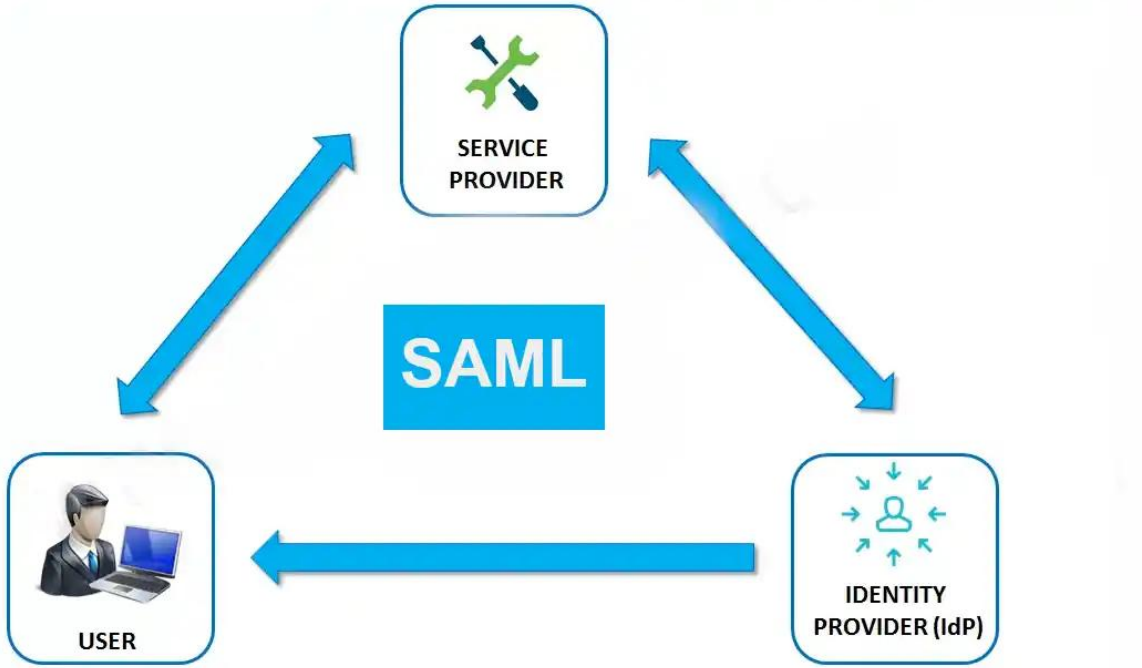
# The way forward



# The way forward

# Claims and attributes

```
<saml:Assertion MajorVersion="1" M
  Issuer="ActAsSts" IssueInstant="2
  <saml:Conditions NotBefore="2015
    <saml:AudienceRestrictionCondi
      <saml:Audience>https://relyi
    </saml:AudienceRestrictionCond
  </saml:Conditions>
  <saml:AttributeStatement>
    <saml:Subject>
      <saml:NameIdentifier>1</saml
      <saml:SubjectConfirmation>
        <saml:ConfirmationMethod>u
      </saml:SubjectConfirmation>
    </saml:Subject>
    <saml:Attribute AttributeName=
      <saml:AttributeValue>Sample
    </saml:Attribute>
    <saml:Attribute AttributeName=
      <saml:AttributeValue>PL</sam
    </saml:Attribute>
    <saml:Attribute AttributeName=
      <saml:AttributeValue>sampleu
    </saml:Attribute>
    <saml:Attribute AttributeName=
      <saml:AttributeValue>Admin</
      <saml:AttributeValue>User</s
    </saml:Attribute>
  </saml:AttributeStatement>
  <Signature xmlns="http://www.w3.o">...</Signature>
</saml:Assertion>
```



# Fast forward to today

- RBAC is here to stay…
  - for the next 20 years…

# Fast forward to today

- Adding dynamic access control capabilities is essential
  - Roles are local and static
  - Non-human identities have no role
  - Roles lack the concept of context, dynamics
    - Roles are attributes

If roles are just attributes, how do we give access?

# Fast forward to today

- Next up: Policy Based Access Control
  - Business rules act on attributes to make the access control decision
  - Dynamics and continuous policy validation are a pre-condition for Zero Trust
    - Identity is just another attribute

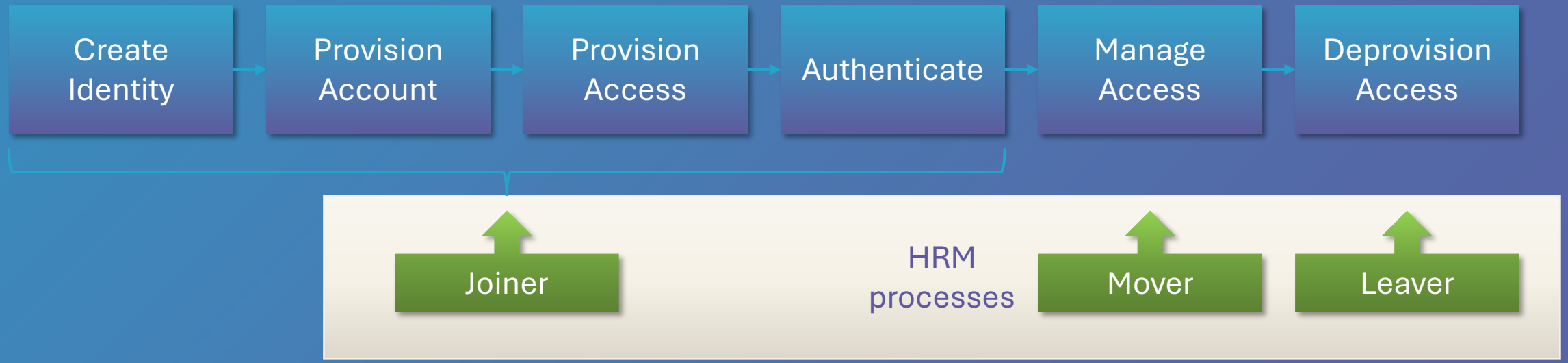
If identities are just attributes, how do we grant access?

# Beware of humans…
## If Identity is just another attribute, then

- good data quality of identity providers is essential
- Joiner – Mover – Leaver processes can be automated
    - Hello IGA!
- we need to know who is involved in a transaction
    - logging and monitoring will become more important
- the concept of objects and subjects becomes more important
    - ‘on behalf of’ is a key concept
    - ‘for the benefit of’ is not yet a well-known concept…
        - we need to identify the transaction-initiating actor

# Lifecycle workforce IAM

IDPRO



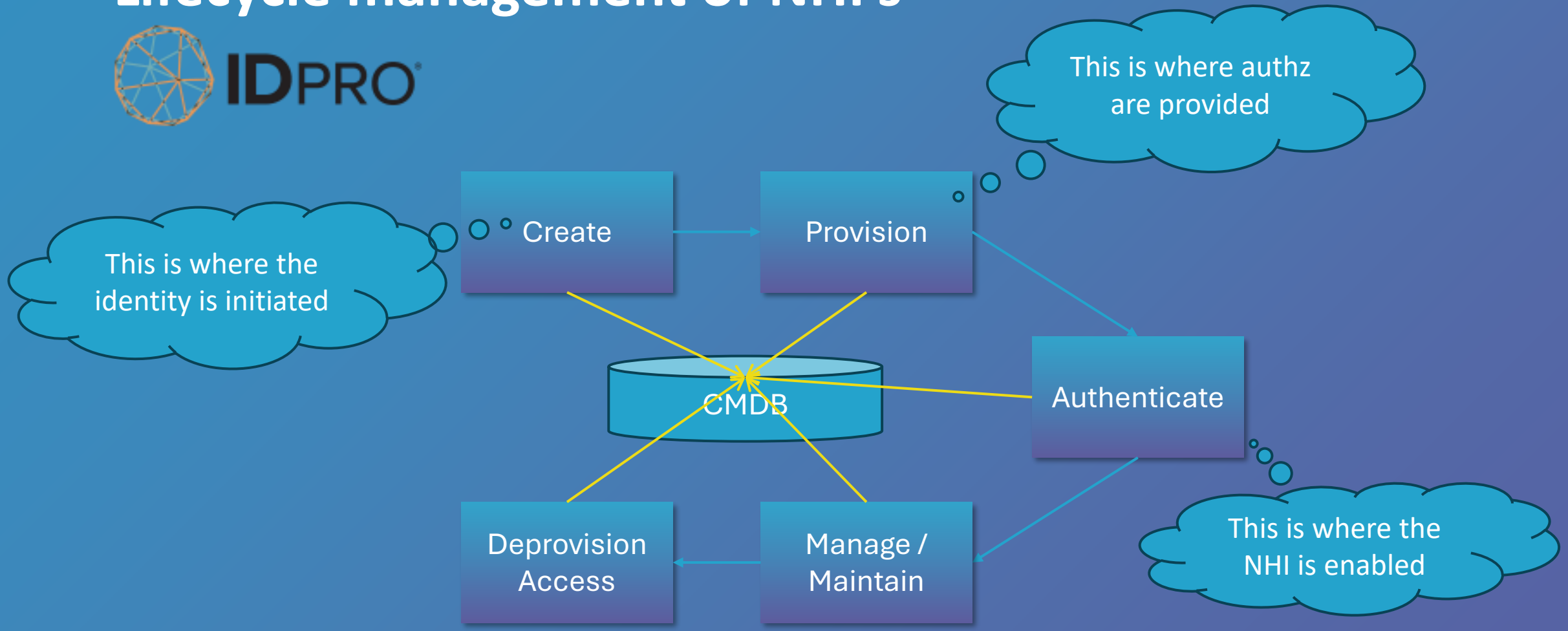

sonicbee


13

# Beware of the non-humans

- Non-Human Identities are different from Human Digital Identities
  - Lifecycle management is key
  - Permission management is hell

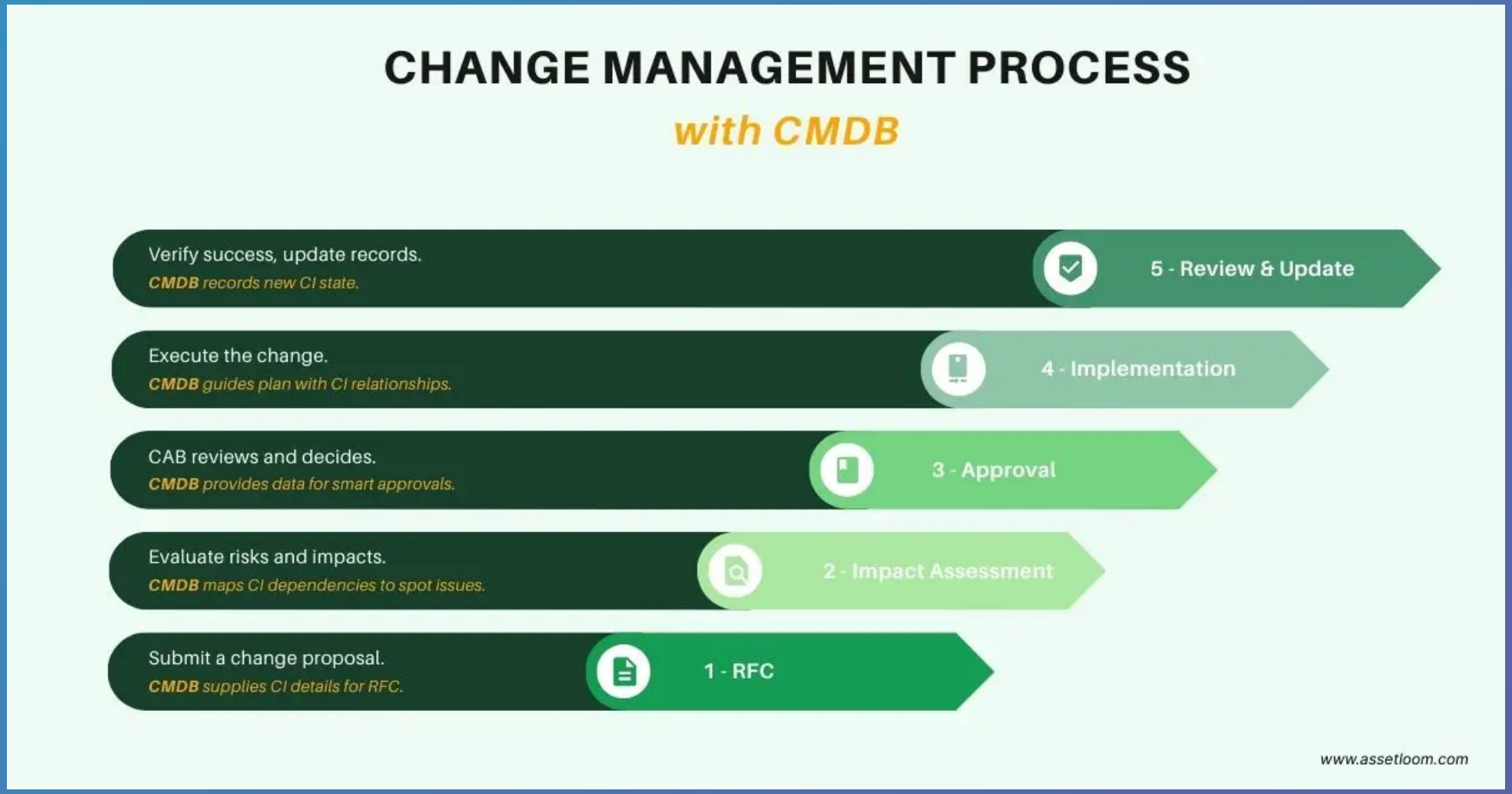
# Lifecycle management of NHI's





15

# Change management. And CMDB…





16

# Human versus non-human identities

IDPRO

| | Person Identity | Non-human Identity |
|---|---|---|
| Usage | Multi-faceted, must accommodate multiple access requirements to many applications or protected resources | Purpose-specific, with a single requirement for each deployment |
| Lifecycle | Created during the 'joiner' process, modified when 'moves' occur, continually monitored for compliance, disabled, and then deleted according to the 'leaver' process. [1] | Created on deployment of the device/service, deleted on termination. |
| Access control | Dynamic – continual risk-assessed authentication matched to the assurance level requirements of the requested application or protected resource. MFA is used for authentication elevation. | Static – determined at the time of account creation. No MFA requirement. |
| Access endpoints | Users typically access computer services from smartphones, PCs, and laptops on an interactive basis. | Endpoints are typically devices or device controllers. They can also be computer applications, service routines, or Internet bots. |

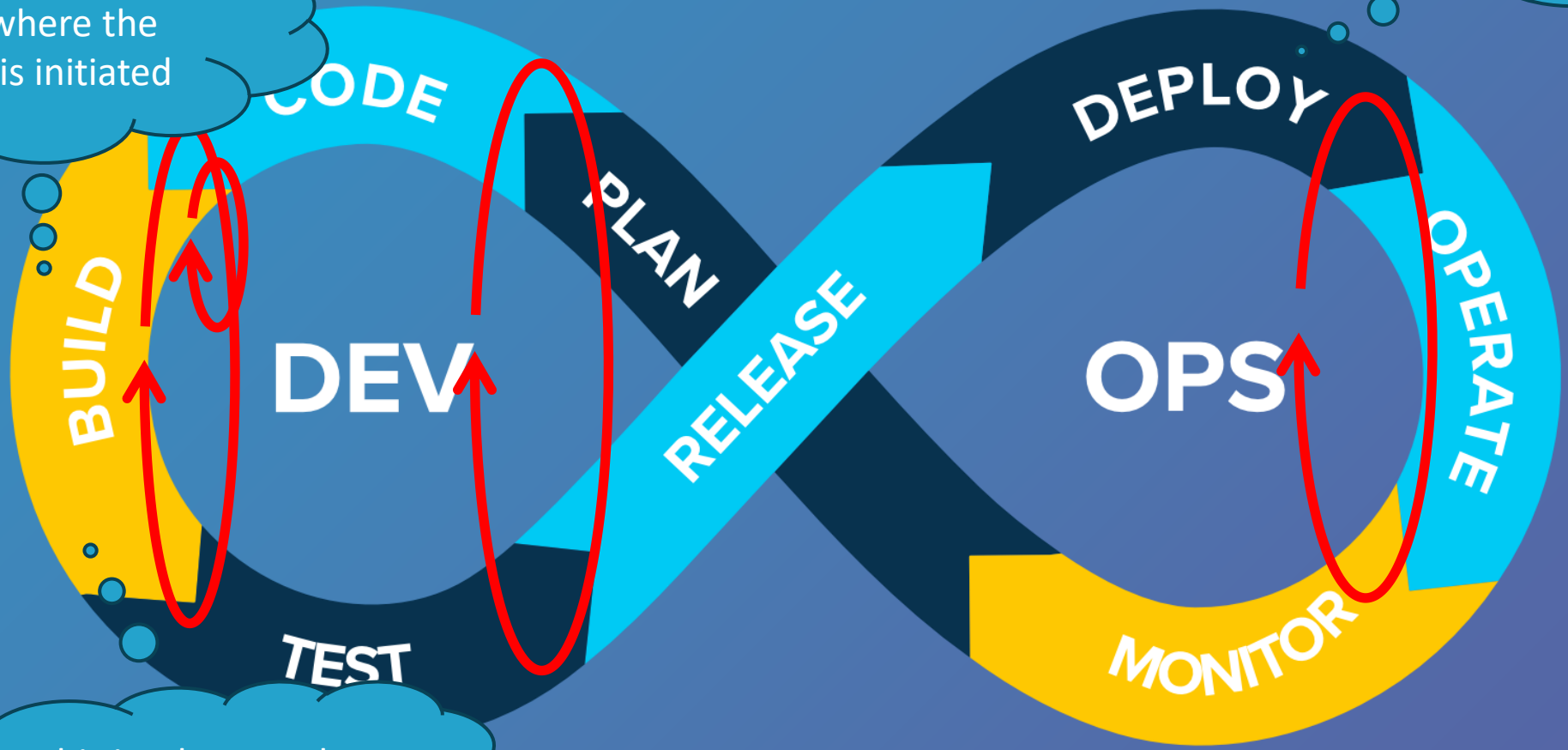
*Table 1 - Account type characteristics*

https://bok.idpro.org/article/id/52/

# Change management in CI/CD

This is where the identity is initiated

This is where the NHI is enabled




This is where authz are provided


18

# AI Agent lifecycle…


- Identity conceived
- Identity created
- Identity enabled
- Identity governed
- Identity removed


19

# Future State of Access

If roles are just attributes, how do we give access?

If identity is not the new perimeter but…
just another attribute, how do we grant access?

We need a new perimeter: Access Governance, Access Policies


21

# And how about NHI access?

Governance

**Who is the owner?**

Every NHI has an owner who is accountable for the NHI actions

**What is the purpose?**

An NHI is created to perform tasks. Specific business tasks.

**How do we identify?**

Manual provisioning is only feasible for manual change management processes...


**What authorizations?**

Not just a role. Dynamic: a rule, taking into account purpose and context.

Trust

# Back to the Future State of Access

Access policies are business rules, working on attributes

Identities are attributes, but needed for accountability

We need new dynamic security / controls. How?

sonicbee


23

# And how about NHI access?

Dynamic Access

**Policy Based Access**

Business Rules define access: SoD, policy resolution and prioritization

**Relation Based Access**

(Trust) relation between hosts define effective access

**Policy Orchestration**

Logical sequential policy flows define the outcome of the access control decision

MECE Access Policy Governance

# Back to today to prepare for your future

SPIFFE/SPIRE, MCP, UMA, CIBA, UTCP
It’s all over IT again. But think again…

Who can have access to what and why is that

It’s all about the business

IGA, PAM, CIAM, SPIFFE/SPIRE, MCP, UMA, CIBA, UTCP, and Access Governance

It’s just too much. IAM can no longer be a one man band.

It requires a TEAM with professionals from business and IT

sonicbee


25

# Kennisevent PAM: bescherm kritieke IT/OT-toegang (NIS2)

22 april @ 11:30 am - 3:00 pm CEST

**Wat begint met gestolen**
**toegang tot kernsysteme**
**continuïteit.**

Security incidenten beginnen vaak k
serviceaccount of een te ruim inges

Het echte risico zit in de schade die
naar privileged access en accounts
OT-omgevingen weet te verkrijgen e

Maar wat als je die toegang achter e
(PAM) helpt om die toegang beheers
is op zichzelf al zeer waardevol en ve


**Gegevens**

**Datum:**

22 april

**Tijd:**

11:30 am - 3:00 pm CEST

**Evenement Categorie:**

SonicBee Kennisevent

**Evenement Tags:**

IT/OT, Kritieke toegang, NIS2, non-human identities, PAM, PAM en NIS2

**Locatie**

./ Dotslash Utrecht
Europalaan 400
Utrecht, Utrecht 3526 KS Nederland
+ Google Maps

**Organisator**

SonicBee

https://www.sonicbee.eu/event/pam-en-nis2-bescherm-kritieke-it-ot-toegang/?lang=nl

# Thank you...


**André Koot**

+31 6 24512021

Andre.koot@sonicbee.eu

Sonicbee

Europalaan 400

3526 KS Utrecht

Netherlands

Identifying Stakeholders in Access Governance

https://www.sonicbee.eu/identifying-stakeholders-in-access-governance/

Meer leuke links:

IDPro Body of Knowledge:
https://idpro.org/body-of-knowledge/

PvIB SIG IAM:
https://www.pvib.nl/actueel/nieuws/nieuw-bij-pvib-special-interest-group-identity-access-management-iam

Webcast:
https://gluu.org/identerati-office-hours-episodes/

Podcast:
https://www.identityatthecenter.com/