THALES
Building a future we can all trust

Thales Identity:
Workforce & B2B

Michael Dybek – Sr. Solutions Consultant (IAM)
www.thalesgroup.com

Agenda

01

Welcome & Opening

5 mins

02

Workforce Access Management

30 mins

03

Access Management for B2B

40 mins

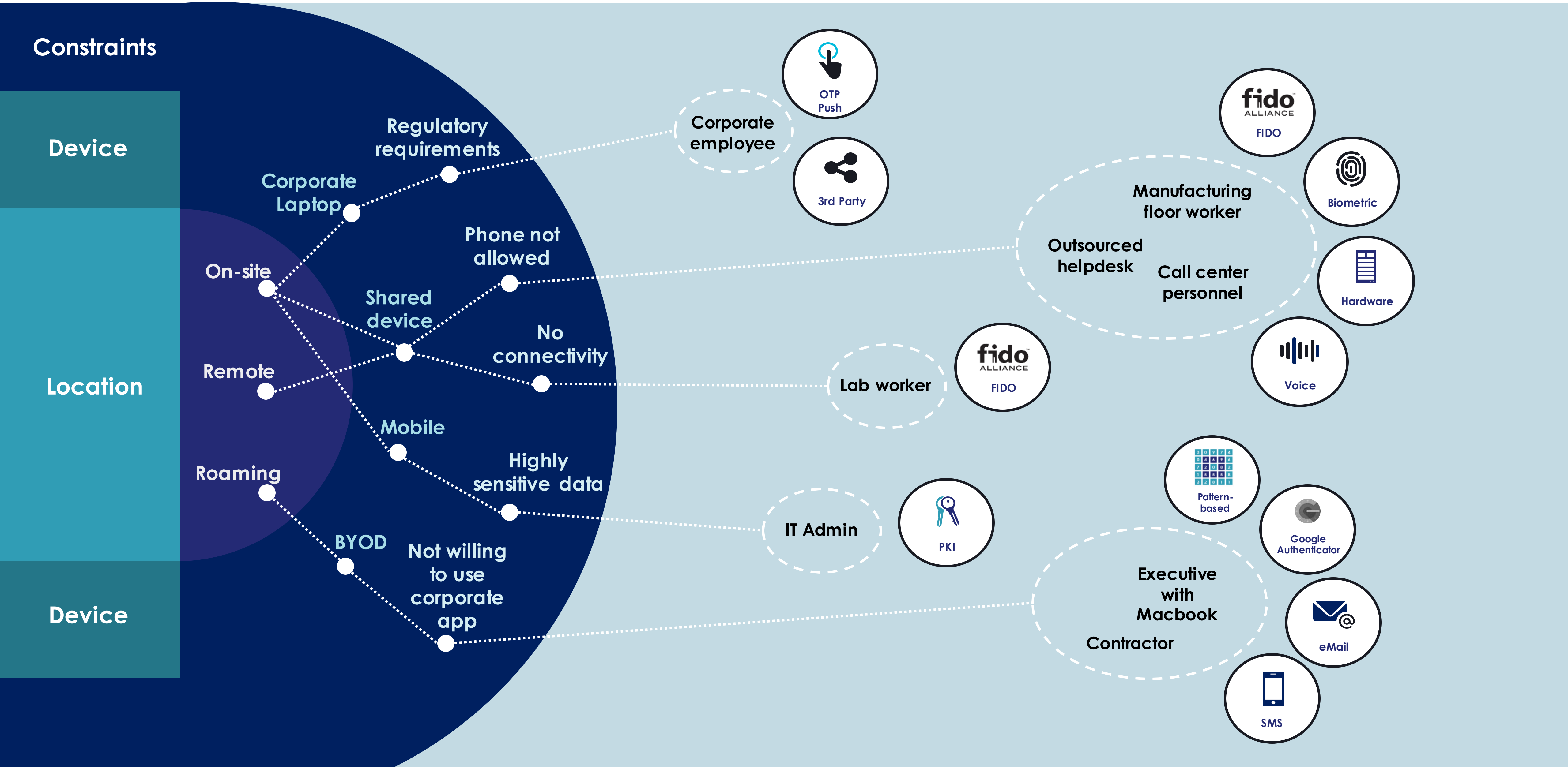
04

Q&A & Closing

5 mins

WORKFORCE ACCESS MANAGEMENT

Different Users, Different Security, Different User Journey



Constraints

Device

Location

Device

On-site

Remote

Roaming

Corporate Laptop

Regulatory requirements

Shared device

Phone not allowed

No connectivity

Mobile

Highly sensitive data

BYOD

Not willing to use corporate app

Corporate employee

Manufacturing floor worker

Outsourced helpdesk

Call center personnel

Lab worker

IT Admin

Executive with Macbook

Contractor

Focus: Authentication For All

- Multiple authentication modules as listed below are available to choose from.

USERNAME + PASSWORD

MAGIC LINK (EMAIL)

MOBILE APP (QR CODE)

SOCIAL LOGIN

EXTERNAL IDENTITY LOGIN

1st Factor Options

Password

SMS

eMail

Voice

Pattern-based

Google Authenticator

Hardware

3rd Party

Kerberos

OTP Push

BYOA

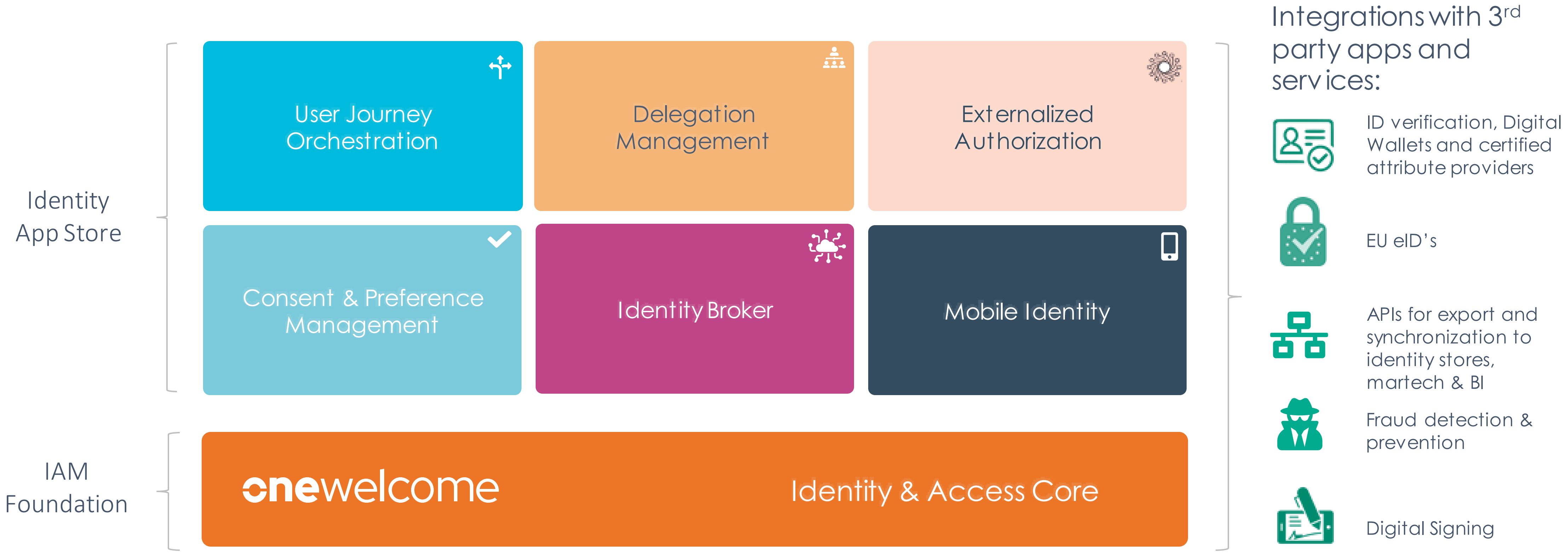
PKI

2nd Factor Options

CONSUMER ACCESS MANAGEMENT

Identity Apps for B2C, B2B & Gig Worker Use Cases

Business identity apps on top of a solid OneWelcome core or augmenting 3rd party IAM



Identity App Store

User Journey Orchestration

Delegation Management

Externalized Authorization

Consent & Preference Management

Identity Broker

Mobile Identity

IAM Foundation

onewelcome

Identity & Access Core

Integrations with 3rd party apps and services:

- ID verification, Digital Wallets and certified attribute providers
- EU eID's
- APIs for export and synchronization to identity stores, martech & BI
- Fraud detection & prevention
- Digital Signing

Differentiators in the Market

User Journey Orchestration

Best suited journey for the targeted user

Consent & Preference Management

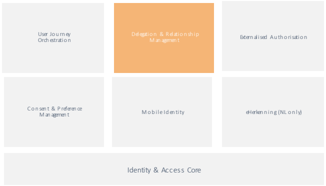
Fully GDPR Compliant

Delegation Management

Delegate user & access management

Externalized Authorization

Complex, fine-grained authorization defined as relationships



User Journey Orchestration

Delegation & Relationship Management

Externalised Authorisation

Consent & Preference Management

Mobile Identity

eHerkenning (NL only)

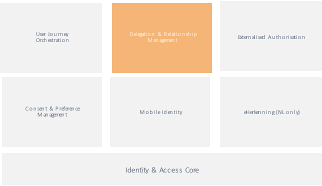
Identity & Access Core

DELEGATION MANAGEMENT

App workflow structure

Delegation Management

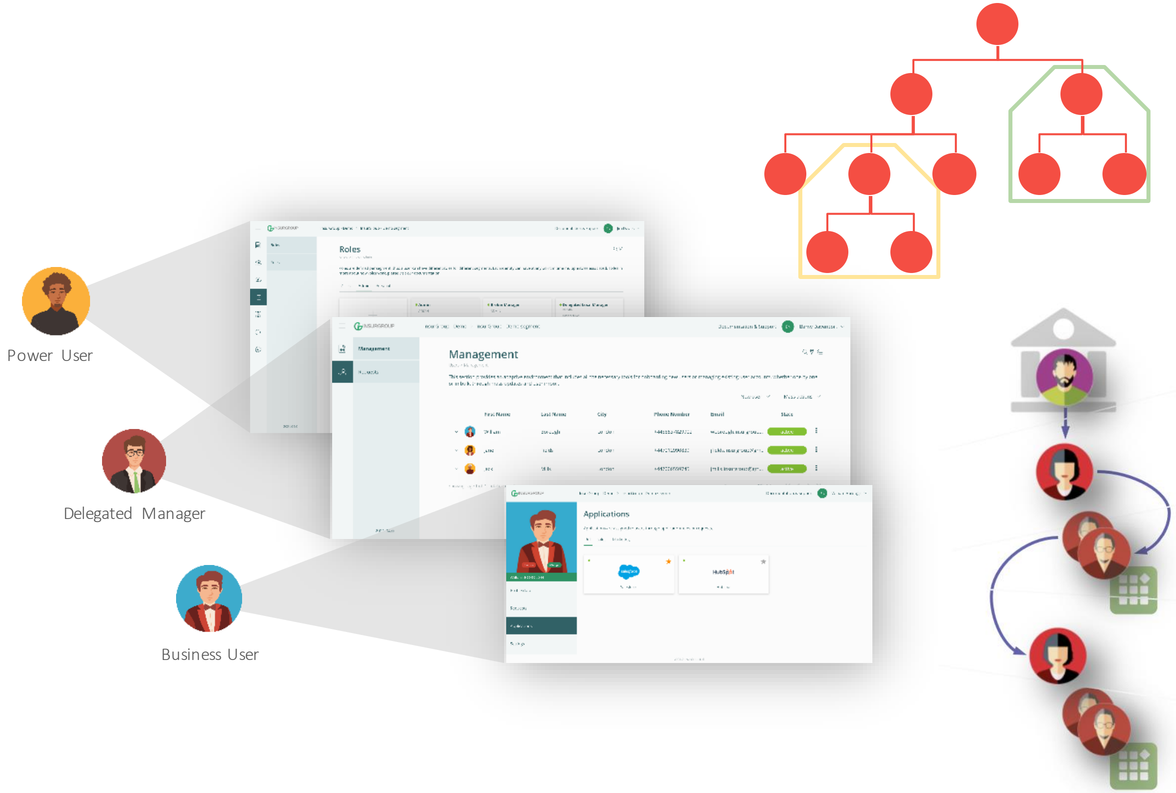
Delegate access and authorisations for online collaboration


User Journey Orchestration
Delegation & Relationship Management
Externalised Authorisation
Consent & Preference Management
Mobile Identity
eHerkenning (NL only)
Identity & Access Core

- Delegate user management to partners and teams
- Invite friends and family to your online service
- Share data with people you trust
- Assign and attest your power of attorney
- Consent on behalf of someone else

Key capabilities

- Deploy canned use cases with out-of-the-box UI or build your own UX with our SDK
- Use graphical modelling tool to define delegations and relationships
- Construct your business context with hierarchies, graph relationships or matrices
- Assign users automatically or manually to roles, groups and relationships
- Write rule syntax to granularly govern delegation, approval and attestation policies
- Integrate with CRM and SIEM platforms to turn events into data



Demo Story

INSURGROUP

ROADHELP SERVICES

BB brokers

INSUR CAR

INSUR LIFE

INSUR HOME

INSUR TRAVEL

INSUR CONTENT

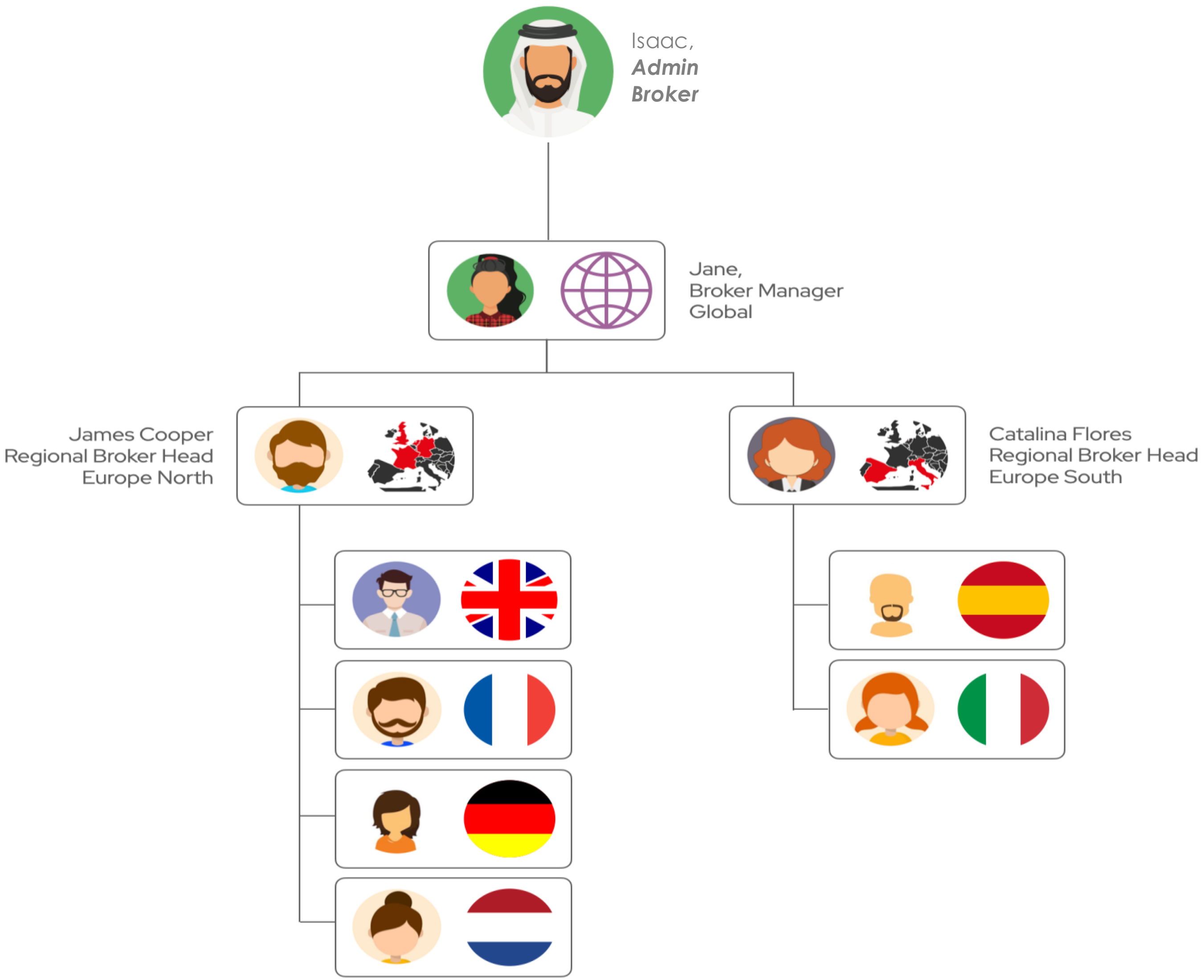
car-surance

- ***Insurgroup*** is an insurance company selling multiple products under different brand names
- ***Insurgroup*** has global partnership with
  - ***Roadhelp***
  - ***BB Brokers***

- ***Roadhelp*** is global mobility company which offers roadside assistance
- ***Roadhelp*** has global partnership with Insurgroup
- ***Roadhelp*** provides roadside assistance in case of vehicle breakdown for Insurgroup consumers with car insurance

- ***BB Brokers*** is global insurance brokerage firm
- ***BB brokers*** has global partnership with Insurgroup
- ***BB brokers*** sells insurance products from Insurgroup globally

BB Brokers - Organigram



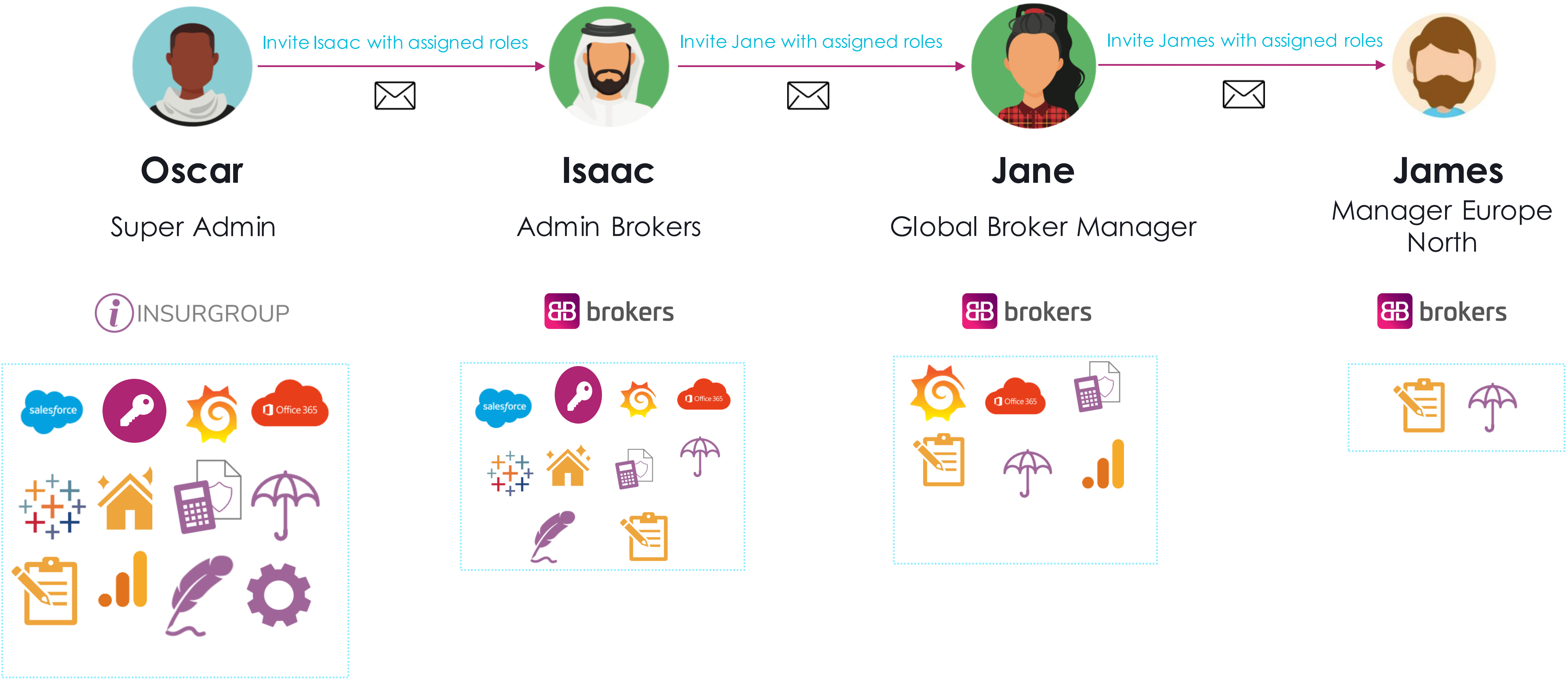
- ***Isaac*** is ***IT Admin*** for Brown Brokers and is responsible for technically managing the set-up

- ***Jane*** is the ***Global Broker Manager*** and supervises all the broker agents

- ***James Cooper*** is the ***Regional Broker Head for Europe North*** and oversees all the broker agents in UK, France, Belgium & NL

- ***Catalina Flores*** is the ***Regional Broker Head for Europe South*** and oversees all the broker agents in Spain & Italy

Delegating Access – What does it look like?



Invite Isaac with assigned roles

Invite Jane with assigned roles

Invite James with assigned roles

Oscar

Super Admin

Isaac

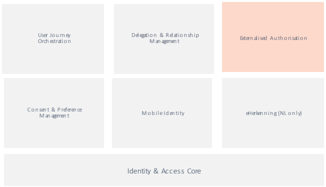
Admin Brokers

Jane

Global Broker Manager

James

Manager Europe North



User Journey Orchestration

Delegation & Relationship Management

Externalised Authorisation

Consent & Preference Management

Mobile Identity

eHerkenning (NL only)

Identity & Access Core

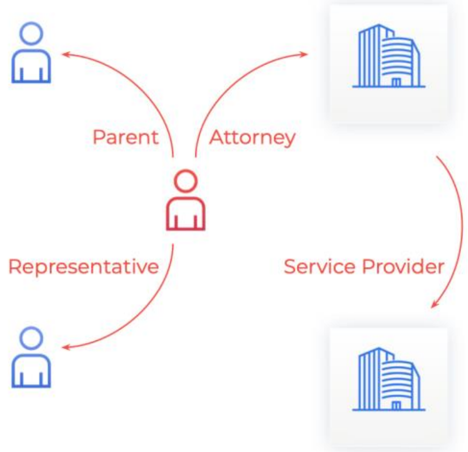
EXTERNALISED AUTHORISATION

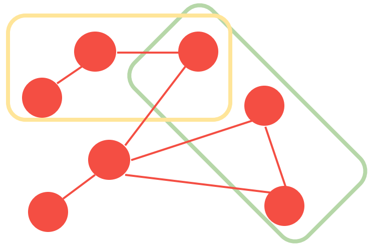
App workflow structure

Externalised Authorisation

Externalise Authorisations with powerful policy editor and enforcement

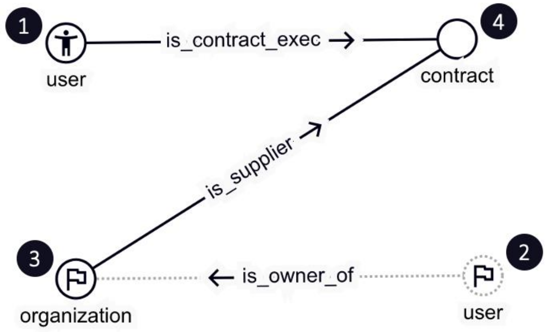
- Manage authorisations for multiple commercial and bespoke application
- Streamline permissions management from a single platform
- Evaluate relationships between users to grant access
- Separate policy management from application lifecycle





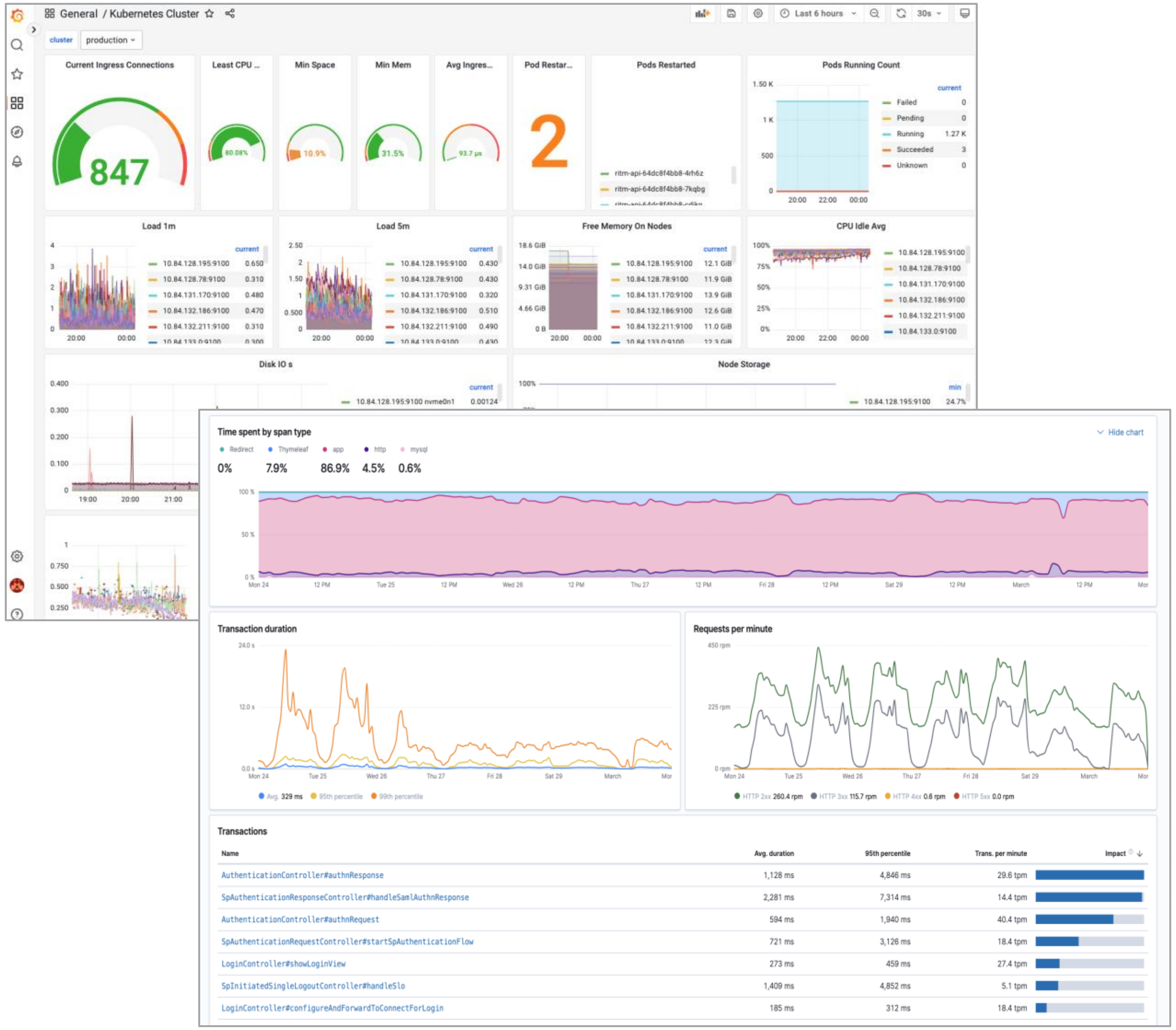
Key capabilities

- Visual editor to start fast with the power of Graph relationship policy modelling
- Evaluate your authorisation policies before tokens are issued or refreshed
- Transport fine-grained authorisation decisions via enriched access tokens
- Optionally, connect your bespoke app back-end to the decision endpoint
- Support for market standards: Open Policy Agent, XACML reference architect, OAuth 2.1



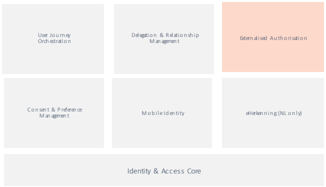
Monitoring for Users

- Continuous monitoring as part of the SaaS offering
- Monitoring of both logs (Elastic Cloud) and metrics (Prometheus & Thanos)
- Any anomaly detected in either logs or metrics leads to Alerts
- Alerts can be integrated with external systems like Opsgenie, Slack, Emails
- Includes outside-in uptime monitoring
- Additional measures like intrusion detection in place



Transactions

Name	Avg. duration	95th percentile	Trans. per minute	Impact
AuthenticationController#authnResponse	1,128 ms	4,846 ms	29.6 tpm	
SpAuthenticationResponseController#handleSamlAuthnResponse	2,281 ms	7,314 ms	14.4 tpm	
AuthenticationController#authnRequest	594 ms	1,940 ms	40.4 tpm	
SpAuthenticationRequestController#startSpAuthenticationFlow	721 ms	3,126 ms	18.4 tpm	
LoginController#showLoginView	273 ms	459 ms	27.4 tpm	
SpInitiatedSingleLogoutController#handleSlo	1,409 ms	4,852 ms	5.1 tpm	
LoginController#configureAndForwardToConnectForLogin	185 ms	312 ms	18.4 tpm	



User Journey Orchestration

Delegation & Relationship Management

Externalised Authorisation

Consent & Preference Management

Mobile Identity

eHerkenning (NL only)

Identity & Access Core

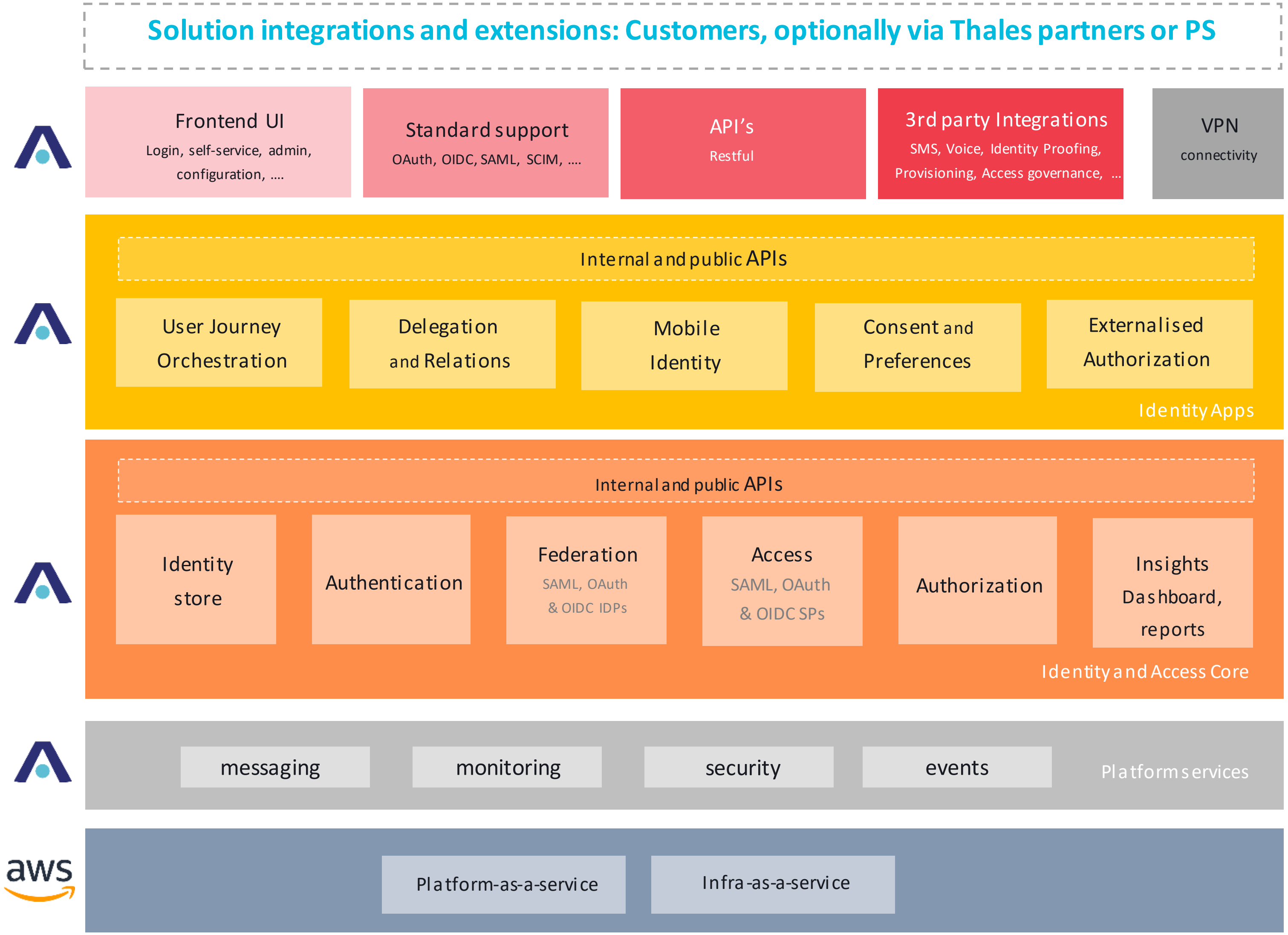
FUNCTIONAL ARCHITECTURE

Solution Deployment

Architecture Overview

Key Facts

- 100% SaaS
- Cloud Provider : AWS (strategic)
- Modern technology stack:
  - Java and JavaScript microservices
  - JavaScript frontend
  - Docker and Kubernetes (EKS)
  - Automated CI/CD pipeline
  - Secure Software Development Lifecycle
- Multi-tenant system
- Everything is built on API first approach



Solution integrations and extensions: Customers, optionally via Thales partners or PS

Frontend UI
Login, self-service, admin, configuration, ….

Standard support
OAuth, OIDC, SAML, SCIM, ….

API's
Restful

3rd party Integrations
SMS, Voice, Identity Proofing, Provisioning, Access governance, …

VPN
connectivity

Internal and public APIs

User Journey Orchestration

Delegation and Relations

Mobile Identity

Consent and Preferences

Externalised Authorization

Identity Apps

Internal and public APIs

Identity store

Authentication

Federation
SAML, OAuth & OIDC IDPs

Access
SAML, OAuth & OIDC SPs

Authorization

Insights Dashboard, reports

Identity and Access Core

messaging

monitoring

security

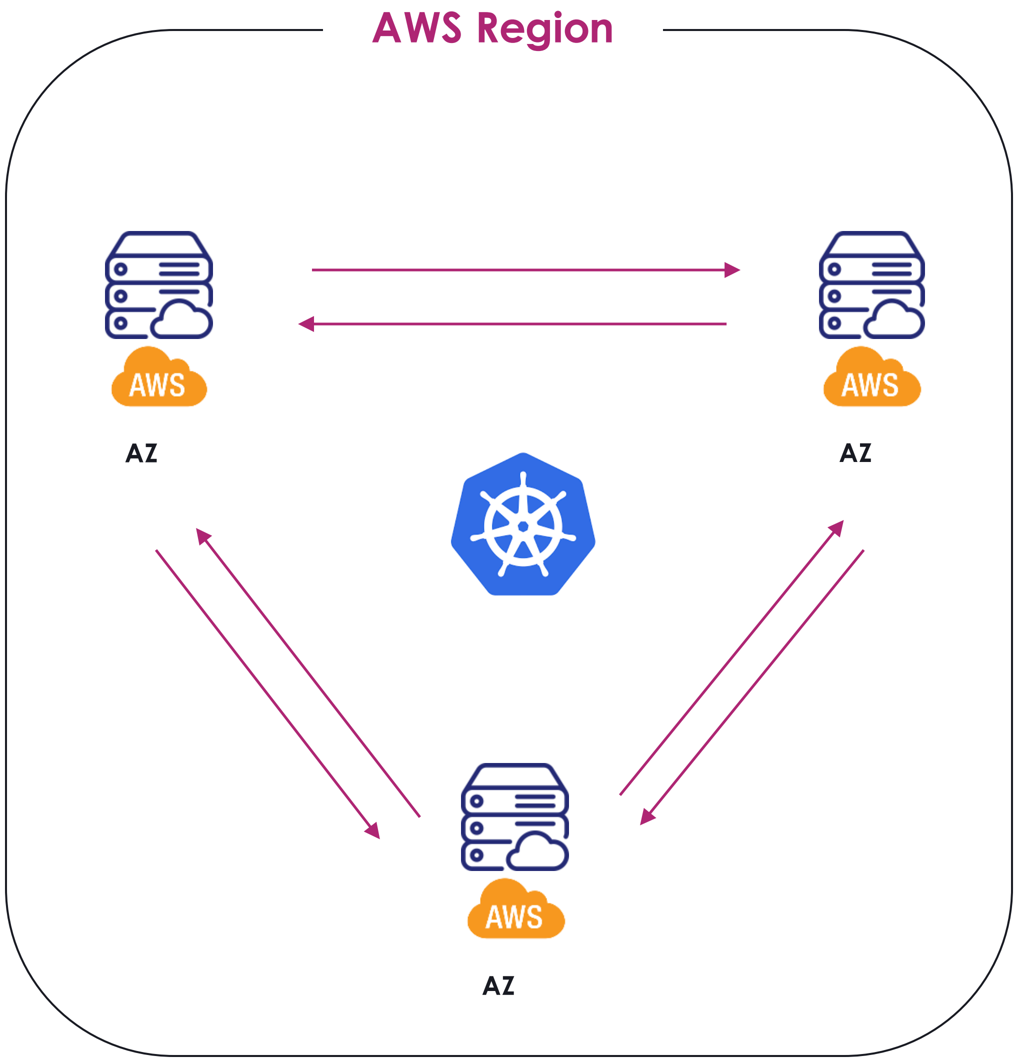
events

Platform services

Platform-as-a-service

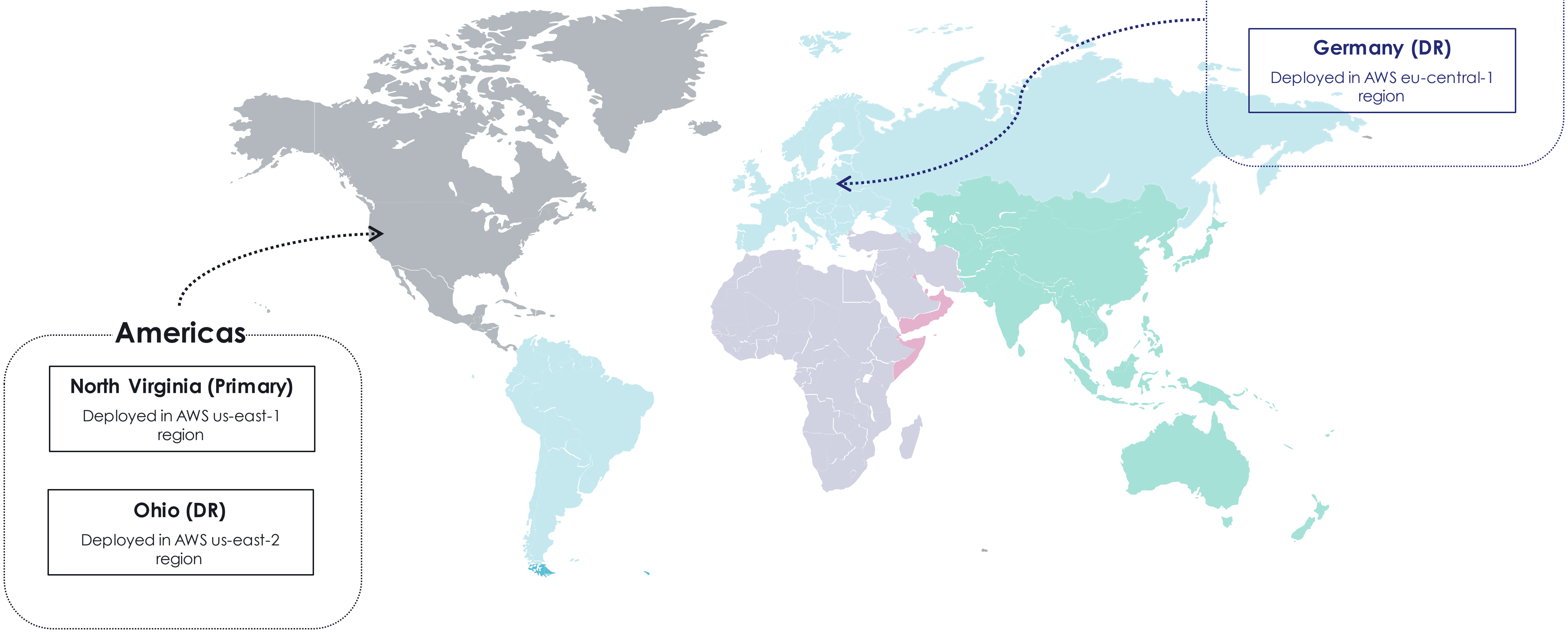
Infra-as-a-service

Availability & Scalability



- Deployment in **3 Availability zones (AZ)** in a region for high availability
- **99.99% availability** in SLA
- Kubernetes **auto healing** to deal with AZ outage within a region
- **2 deployments regions** for every customer –
  - Primary
  - DR (Disaster Recovery)
- Near **unlimited scalability** with AWS & Kubernetes

Deployment Regions



EU

Ireland (Primary)

Deployed in AWS eu-west-1 region

Germany (DR)

Deployed in AWS eu-central-1 region

Americas

North Virginia (Primary)

Deployed in AWS us-east-1 region

Ohio (DR)

Deployed in AWS us-east-2 region

*Security measures are part of the commitment, not the tools, thus tools can change over time

Data Encryption

> Encryption at Rest

- > All the data at rest is encrypted
- > Encryption is done using the AWS KMS
- > For multi tenant services, different keys are used to encrypt the data for each customer

> Encryption in flight

- > All the data in transit on internet is encrypted
- > *TLS 1.2 & 1.3 supported*

Back-up & Disaster Recovery

> Back-up

- All data backed up daily
- Backups are encrypted with tenant specific keys at rest using AWS KMS, AES-256-GCM
- Backups are replicated to DR region and stored for 30 days
- Service to decrypt the data can only be access by authorized Thales's personnel

> Disaster Recovery

- DR location assumes the primary responsibility in case the primary region has outage
- Backup restore is tested at least once per year as part of the DR process
- DR procedure is also tested at least once per year as part of the SOC2 Type2 compliance

Compliance & Certification

onewelcome
a Thales company

SOC 2 Type II Report

Thales OneWelcome Identity Platform

System:	OneWelcome IDaaS
Description:	ISAE 3000 / Service Organization Control Report, type 2, based on SOC 2® report model (2018) and the Trust Services Principles and Criteria (2017) for Security, Availability, Confidentiality and Privacy
Reference:	2C-2022-395
Report Date:	November, 1st 2022
Audit Period:	July 1st, 2021 until June 30th, 2022
Version:	1.0
Document owner:	CISO
Status:	Final
Classification:	OneWelcome Highly Confidential

SOC 2 Type II

> SOC2 Type II is an evaluation of operation effectiveness over time

ISO 27001

> Assesses protection of sensitive information's confidentiality, integrity and availability in information management systems

GDPR

> Regulates processing of personal data in EU

THALES
Building a future we can all trust

Thank You

Michael Dybek

Sr. Solutions Consultant (IAM)

☎ +44 7513706410

✉ michael.dybek@thalesgroup.com