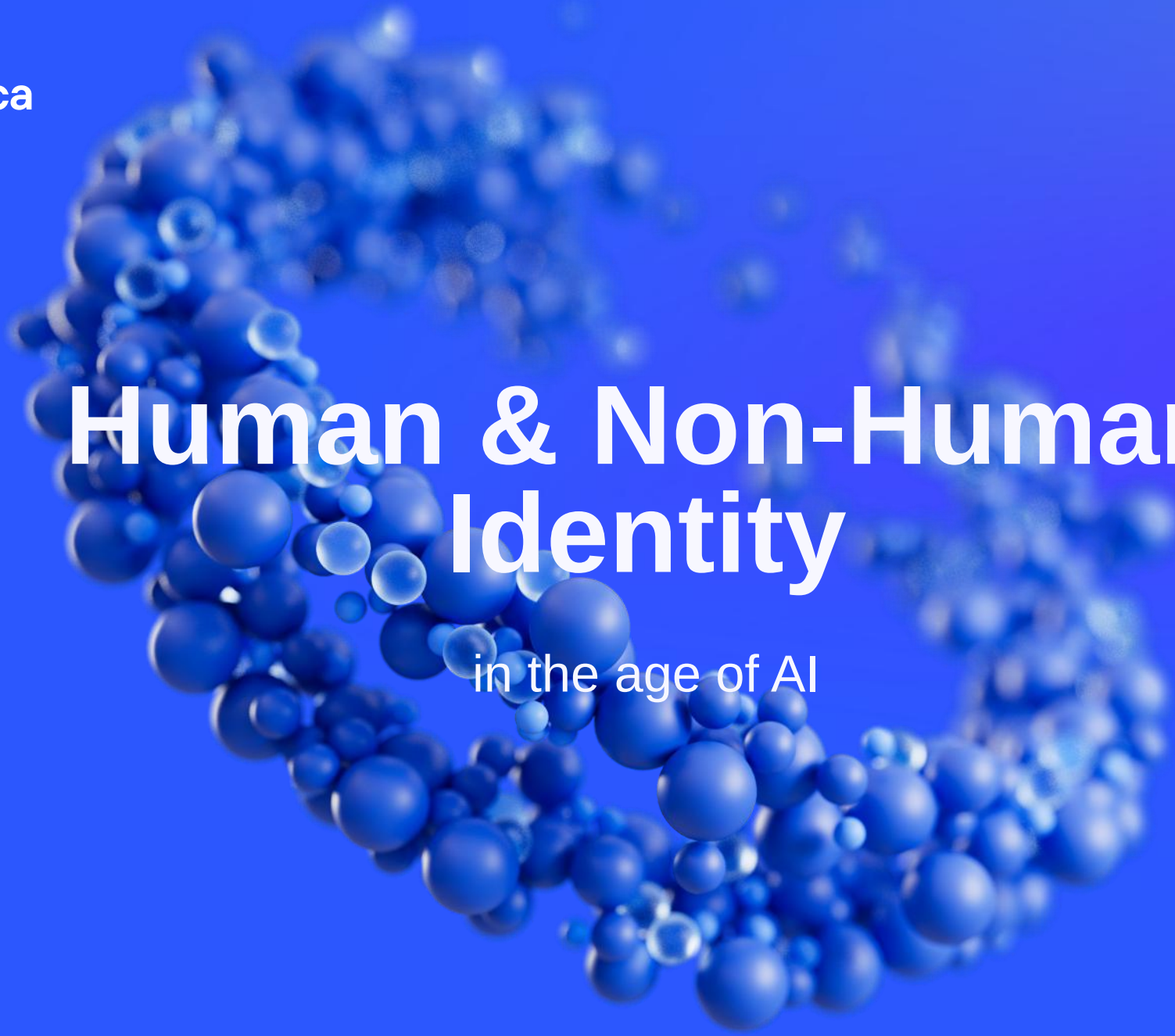
Telefónica

Ready for Next



Human & Non-Human Identity

in the age of AI

Our Speakers

David Prieto Marqués

Head of Identity, Data & AI Security

Telefónica Tech

Inmaculada César Benavides

Director of Media and Technology

tirea

There is no trusted AI without trusted identity

Identity as the control plane of digital trust

Who controls
in an AI-driven world?

Decision

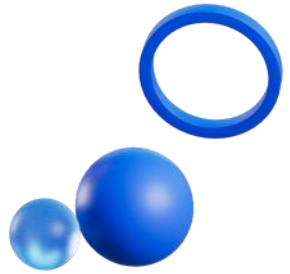
AI is making decisions faster than humans can supervise.

Responsibility

Trust collapses when action cannot be attributed.

Identity

Only identity can anchor access, policy and accountability.



Trust shapes Economies

Identity Shapes Trust

Social

Economic

Systemic

850

million people

Legal identity

850 million people still lack a legal identity, limiting access to services, rights and participants in the digital.

(WEF/World Bank)

Mobile identity

Mobile identity is a critical enabler of digital inclusion, helping close identity gaps at population scale.

(GSMA)

Trust shapes Economies

Identity Shapes Trust

- **Social**
- **Economic**
- Systemic

3-13%

increase of national GDP by 2030

Digital identity

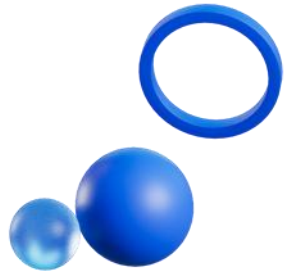
Digital identity could unlock between 3% and 13% of national GDP by 2030 driven by inclusion, efficiency, reduced fraud and trusted digital transactions.

(McKinsey, 2025)

Mobile ecosystem

Trusted digital identity enables new digital services and business models across the mobile ecosystem.

(GSMA)



Trust shapes Economies

Identity Shapes Trust

- **Social**
- **Economic**
- **Systemic**

identity

is a foundational layer

Foundational layer

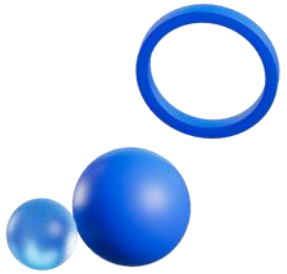
Identity is a foundational layer for trusted digital services, public infrastructures and global digital ecosystems.

(McKinsey, 2025)

Mobile industry

The mobile industry plays a key role in advancing digital trust, providing secure, interoperable identity capabilities at global scale.

(GSMA)



Everyone needs identity, Everyday and for Everything

Identity in the era of AI agents will play a fundamental role in data security and integrity

Trends
IAM

Identity Fabric - Identity in the era of AI agents will play a fundamental role in data security and integrity.

Integrated and Automated IAM Core Capabilities

Strategic Business & Trust Enabler

Trusted Identity as the Foundation for Secure AI

Disruptive Innovations Reshaping IAM Infrastructure

Identity Platform for Humans, Machines and AI Agents

Identity as an Operated Control Plane

Identity-Driven, Architecture

Strategic Business
& Trust Enabler

01.

The Challenge

Identity and Access Management
as **security**

02.

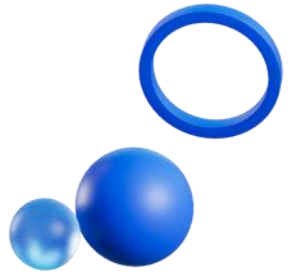
The Transition

Identity and Access Management
as **enabler**

03.

The Solution

Identity as a Business
and **trust** platform



01.
The Challenge

Identity and Access Management as **security**

Tool centric access management

MFA, SSO and RBAC implemented as isolated controls, mainly for audit and compliance.

Limited Scope for emerging identities

Focused on human identities, poorly integrated with business platforms, and unprepared for decentralized identities, machines, AI agents and quantum challenges.

Example 01
Reactive, human-centric and perimeter based.

Example 02
High operational friction.

Example 03
Not designed for decentralization or crypto-agility by design.

02.
The Transition

Identity and Access Management
as **enabler**

Identity expands beyond security

Identity and Access Management evolves into a cross-functional enabler of collaboration, user experience and trust at scale.

Digital identity as a central enabler

Connecting people, machines, AI agents, devices and digital services through a trusted interconnected ecosystem.

Identity as
enabler

03.
The Solution

Identity as a Business and **trust** platform

Identity evolution

Identity evolves from an enabler into a programmer, operated platform that governs all identity types across digital ecosystems.

Unified identity platform

Enterprise users, customers, citizens, machines and AI agents are managed through a unified identity platform that translates business, regulatory and security policies into real-time, enforceable controls.

A unified platform

Can trust really scale across every identity humans, machines and AI?

One identity fabric, operated as a trust platform

Platform Pillars

Universal identity coverage

From each Edge Operator Platform, the federation is established with the rest of the partners.

Policy-Driven authorization

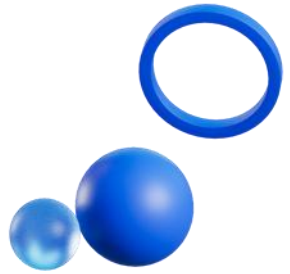
Business policies enforced in real time.

Crypto-Agility and sovereignty

Resilient identity across providers and regulations.

Ai-Native Operations

Automated governance detection and response.



Identity and Access Managament for Insurance Ecosystem Partners

tirea

01.
The Challenges

The **insurance ecosystem** identity challenge

A highly regulated but interconnected ecosystem

Insurance operates under **Solvency II** and **DORA**, which place **digital operational resilience** at the center of the sector.

The insurance value chain depends on **external collaborators not subject to DORA regulation:**

Brokers and agents
Loss adjusters
Repair networks
Hospitals
Lawyers
Service providers

Current Reality

These participants need **daily access** to **multiple insurers' systems:**

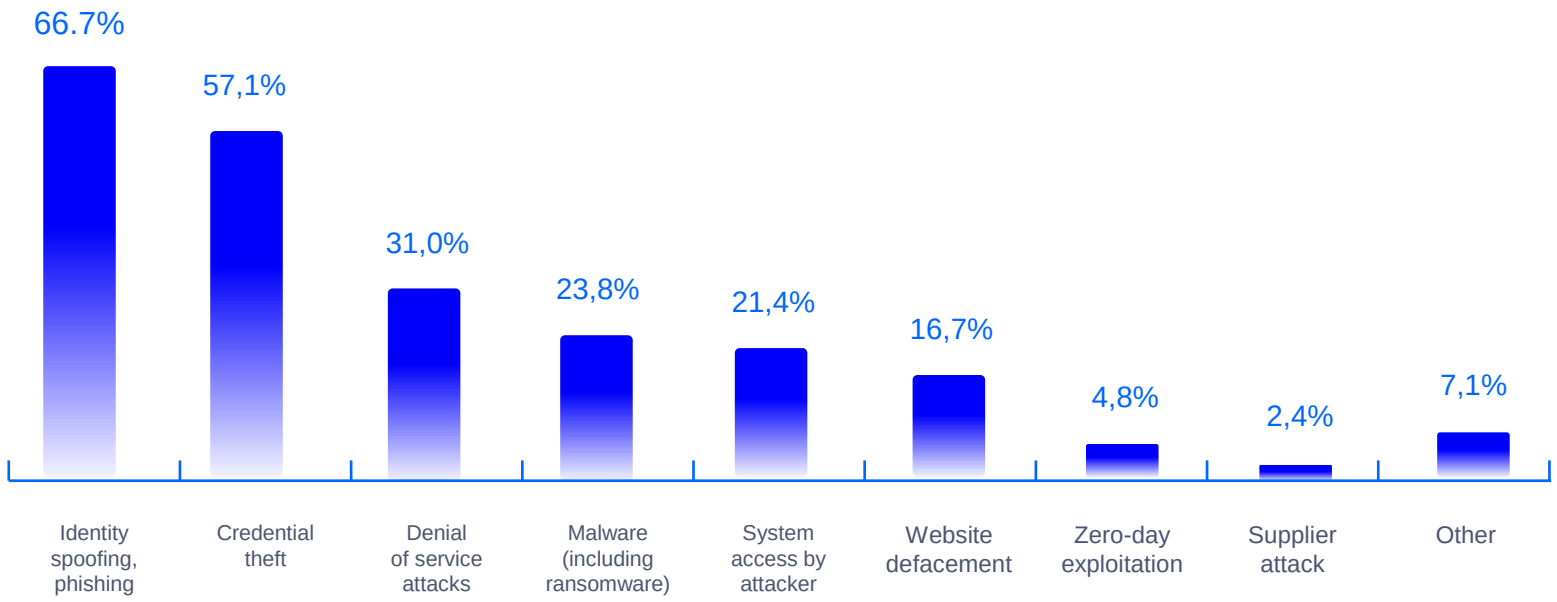
Shared and reused credentials
Fragmented identity management
Limited traceability and governance

The Impact

Identity impersonation and third-party credential theft have become the **main attack vector against insurers.**

01.
The Challenges

Most common cyberattack vector in insurance industry



External identity represents the highest risk

66.7%

Experience Identity Spoofing (Phishing)

57.1%

Experience Credential Theft

This risk is amplified by the fragmented management of external collaborators across the value chain.

01.
The Challenges

Identity Hub

Multiple Credentials:

External collaborators manage different usernames and passwords for each insurer, often including shared or generic accounts.

Inconsistent Security:

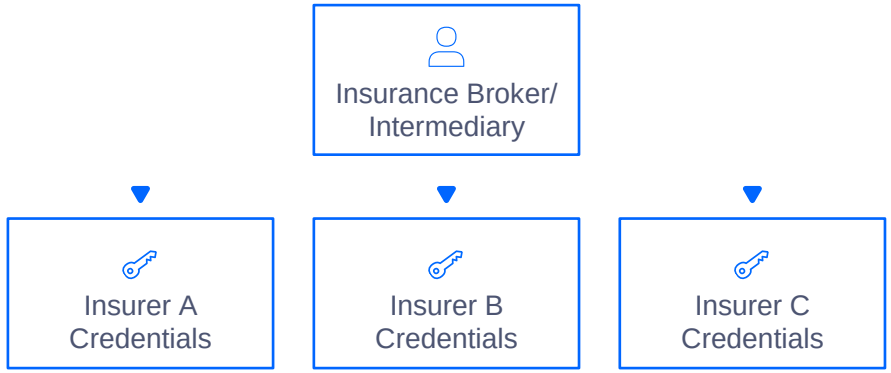
Heterogeneous security policies and varying levels of protection.

Dispersed Processes:

Each entity maintains its own onboarding, offboarding and user management systems.

Compliance Challenges:

Complexity in ensuring regulatory requirements are met consistently across the ecosystem.



A typical broker manages between 5 and 15 different sets of credentials.

Today’s fragmented model drives operational inefficiencies, higher support costs, and greater security exposure across the insurance ecosystem.

02.
The Transition

Identity evolves from a security control to a sector enabler

The insurance ecosystem is evolving toward a shared trust model.

In this model identity becomes interoperable across insurers, centrally governed, lifecycle-managed, policy-driven, and operated at sector level to ensure consistency, security, and scalability.

Identity becomes the control plane for ecosystem trust.

Key shifts

In this model identity becomes interoperable across insurers, centrally governed, lifecycle-managed, policy-driven, and operated at sector level to ensure consistency, security, and scalability.

From siloed identities	→	**interoperable identities.**
From local access control	→	**shared trusted frameworks**
From manual onboarding	→	**centralized onboarding**
From reactive compliance	→	**compliance by design**

02.
The Transition

Transforming fragmentation into unified identity through an Identity Hub

Current situation
Fragmentation

- Multiple Credentials
- Heterogeneous Processes
- Inconsistent Security
- Complex Compliance

With an identity hub
Unification

- Centralized identity
- Standardized Processes
- Strengthened Security
- Simplified Compliance

03.
The Solution

Strategic vision: a centralized, federated, and sovereign identity.

> **This project is a strategic cornerstone for the digital transformation of the insurance sector, built on digital identity, trust, and compliance.**

Centralised

Unified and simplified management under common policies

Fast deployment and direct control by TIREA

Efficient and seamless integration for collaborators

Federated

Unified access to multiple services (SSO)

Interoperability across external collaborators and entities

Shared trust framework

Sovereign

Operational sovereignty and control over identity data

Regulatory compliance under local guarantees (DORA…)

Identity as a sector-wide capability led by TIREA

tirea

03.
The Solution

Differentiating values that make Telefónica Tech's solution unique.

Key Advantages of Telefónica Tech

Security

Guaranteed Security and Regulatory Compliance

Telefónica Tech ensures compliance with frameworks (GDPR, DORA, ENS) through high cybersecurity standards and full traceability.

Trust

High Availability & Scalability by an Infrastructure Leader

Ensures a robust, always-on platform designed to scale in line with the evolving needs of the insurance sector.

Adoption

Agile & Standardized Integration

Enables full interoperability through secure APIs and standard protocols, simplifying integration

A Sovereign and Federated Identity Platform for TIREA, hosted and operated by Telefónica Tech

03.
The Solution

Key strategic objectives

Unify Identity Management

Centralize **the nominal digital identity** of all external collaborators interacting with multiple insurers into a single platform.

- Single Sign-On
- Unified Identity
- Self-Service

Strengthen Security

Implement **uniform security policies** to raise the level of protection across the entire insurance sector.

- Adaptive MFA
- Professional Verification
- Secure Identity Lifecycle

Facilitate Regulatory Compliance

Provide a **common framework** enabling all entities to meet current regulatory requirements.

- GDPR/LOPDGDD
- DGSFP Regulations
- Dora
- eIDAS

03.
The Solution

Applicable Regulatory Framework

GDPR & LOPDGDD

Granular consent management, ARSULIPO rights, access traceability and data minimization.

DORA

Digital operational resilience, security controls based on ISO 27001 and ENS, continuous monitoring.

DGSFP

Automatic verification with the DGSFP PUI, continuous status validation and professional accreditation.

eIDAS / Law 6 /2020

Support for high-trust digital identity, electronic signature and future integration with the EUDI Wallet.

How the Platform Enables Compliance
Identity Hub

- Automated verification with official sources (DGSFP)
- Centralized GDPR consent dashboard
- Full action traceability (auditable logs)
- Homogeneous security controls (Adaptive MFA)
- Standard identity protocols (OIDC, SAML)

The platform reduces regulatory compliance effort for insurers by centralizing controls and oversight.

03.
The Solution

Sector-wide benefits and strategic impact

Operational Efficiency & Cost Reduction

- Lower identity and IT support costs
- Reduced duplication of systems
- Faster onboarding through automated processes
- Streamlined credential and access management

Enhanced Security & Governance

- Adaptive multi-factor authentication (MFA)
- Centralised access and incident response
- Consistent enforcement and security policies
- Simplified compliance and auditing

Improved User Experience

- Single Sign-On (SSO) across insurers
- Unified self-service portal

Future-Ready Innovation

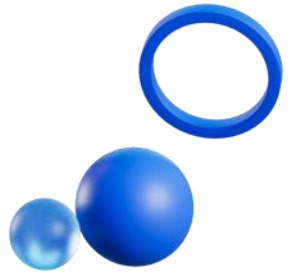
- eIDAS 2.0 and EUDI Wallet readiness
- Extensible architecture for future integrations
- Digital services enablement

What are the two key challenges adressed by our strategic evolution?

tirea

01. **Converging with the eIDAS Digital Identity Wallet** to bridge public and sector identities.

02. **Enabling AI agents** to engage the platform with unified governance of both human and AI identities.




Telefónica