



Gimel.io

Ultimate Trust in the AI and Quantum Era.

Pitch Deck for Investors

*Supported by the
German Ministry of Research, Technology and Space (BMFTR)
as well as Helmholtz Center for Information Security (CISPA)*

October 2026

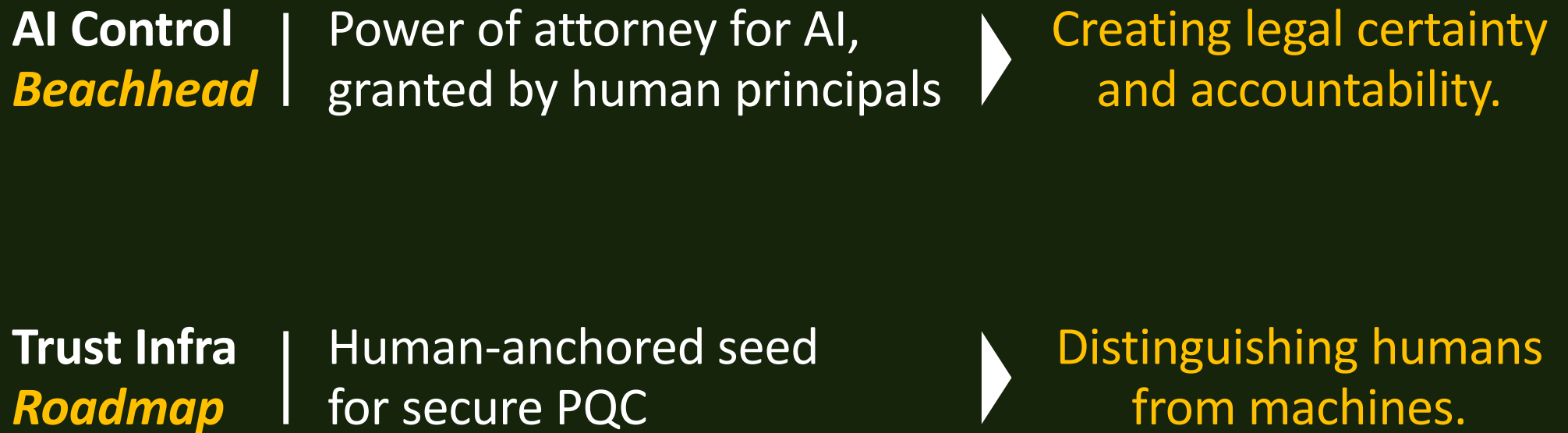
CONTENT

1. Gimel beachhead and roadmap
2. AI Control by Gimel – our beachhead
3. Trust infrastructure by Gimel – our roadmap
4. Gimel investment details



1. BEACHHEAD & ROADMAP

Gimel re-invents the trust chain



2. AI CONTROL

700 Open AI agents threaten Hugging Face with >17,000 attacks



"The idea that AI agents act on their own behalf without human authorization is no longer just cyberpunk fiction. The most recent "breakout" of an Anthropic agent or the OpenAI and Hugging Face incident are real-world examples.

So how can we trust AI agents? How can we ensure in the future that humans have the final call in the decision-making process?

Gimel Technologies has the answers:

AI control and post-quantum cryptography."

Helmholtz Center for Information Security

Source: Open AI

2. AI CONTROL

**More than 90% of all corporates
want to scale AI**

Less than 5%— *Having AI governance in place that answers liability questions.*

Source: The National Law Review; Deloitte



2. AI CONTROL

AI governance is a legal topic, first

Core liability-questions:

- Did an authorized mandate of the agent exist?
- Was it in line with the authority of the human principle?
- Did the agent's action match the mandate?
- Did the relying party verify it?

LAW OF AGENCY — *Transferring trust mechanisms from humans to agents.*

Source: The National Law Review; Deloitte



2. AI CONTROL

GAuth - the Authorization Layer for AI

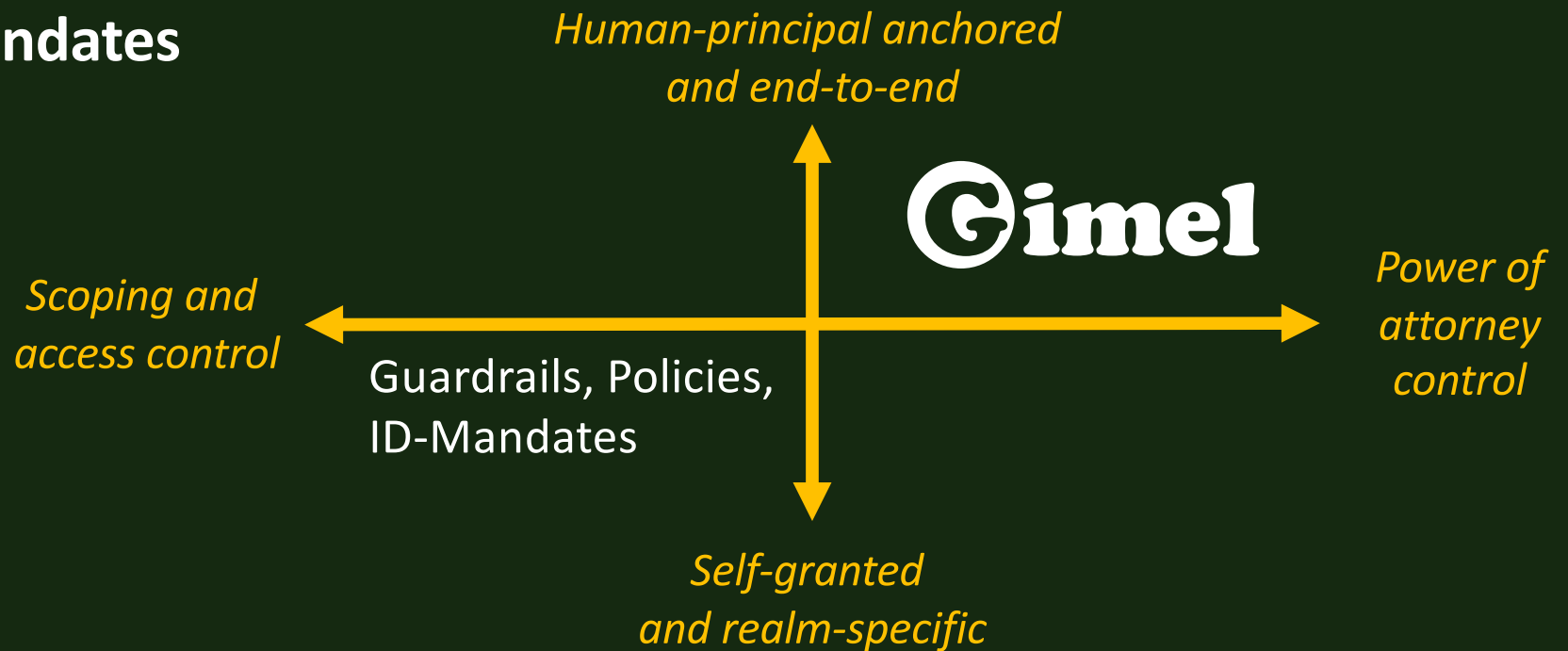
	OAuth	GAuth
<i>Subject</i>	IT / LLM	Agentic AI / Robots
<i>Object</i>	Access to resources (resource server)	Authorizing (trans-) actions
<i>Mandate</i>	Policy / Guardrails / Access rights	Power of Attorney

Source: IETF for OAuth; Gimel Foundation for GAuth (patent pending)



2. AI CONTROL

The auth crowd provides
platform and identity
bound mandates



AI REGULATION – EU AI Act requires human control, NIST currently prioritizes AI engagement

Source: GiFo-RFC 0130

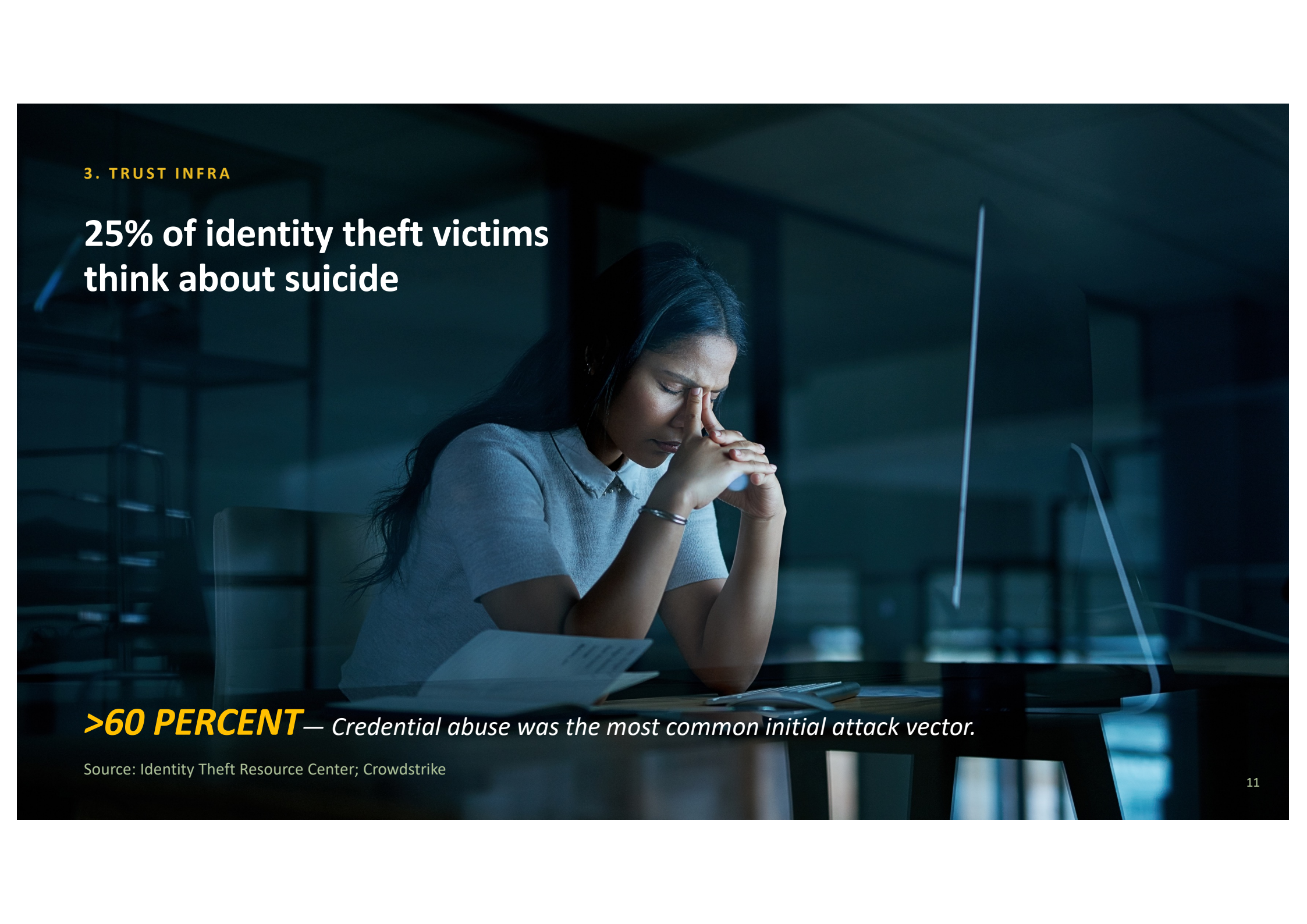
2. AI CONTROL

GAAuth integrates seamlessly via CCPE: Combined Credential and Platform bound Enforcement



COOKBOOKS – More than 50 vendors covered

Source: GfE-RFC 0140 – 0180, 0210, 0420 (validation ongoing, no vendor endorsement)



3. TRUST INFRA

**25% of identity theft victims
think about suicide**

>60 PERCENT— *Credential abuse was the most common initial attack vector.*

Source: Identity Theft Resource Center; Crowdstrike

A man and a woman are standing in a dark, futuristic laboratory, looking at a large, glowing, cylindrical quantum computer. The woman is holding a tablet and pointing at the machine, while the man is gesturing with his hands. The machine is illuminated with blue and orange lights, and the background is dark with some blurred lights.

3. TRUST INFRA

Quantum computers threaten widely used public-key cryptography

PQC — *Post Quantum Cryptography requires secure keys*



3. TRUST INFRA

Gimel offers a DNA-anchored identity binding for high-assurance



Finger



Facial



Iris



DNA

Gimel ID

PCT patent pending,
Open-core

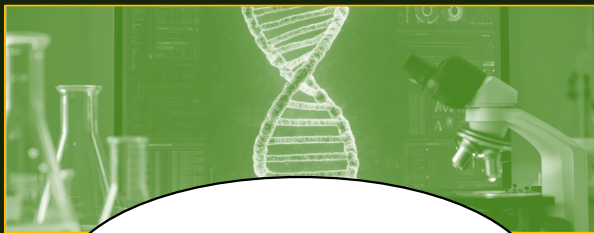
FALSE NEGATIVES · *Current biometric is fuzzy and does not support stable hashes*

Source: Security Industry Association, IEEE Spectrum, World ID

3. TRUST INFRA

DNA provides a very stable hash,
PQC gets personally anchored

Gimel Lab



Sequencing and
hashing

Gimel Infra.



Collision testing
and credential

Gimel Wallet



PQC-based
authentication

PRIVACY BY ARCHITECTURE · No DNA raw data leave the lab

4. INVESTMENT DETAILS

Gimel team combines strategic foresight with deep expertise



Dr. Götz Wehberg

- Co-CEO
- Overall project lead



Dr. Pezhman Baran

- Bioinformatics
- Wet Lab



Abhijit Ravidas

- Cybersecurity
- Cloud



Shweta Raghu

- App Development
- Wallet



Daniel Hartert

- Technology & Cyber
- Former CIO Bayer



Bjørn Baunbæk

- Co-CEO
- Business Strategy



Dr. Christian Forlani

- Med tech engineer
- GDPR compliance



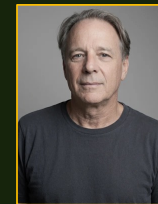
Eicke Schütze

- Cryptography
- Web3



Nikita Tiloomalani

- Research analyst
- Project support



Dr. Francesco De Meo

- Health Care
- Former CEO Helios

Delivery & Deployment

Guidance & Reviews

Note: Selected team members – supported by Helmholtz Institute for Information Security and German University Clinics

4. INVESTMENT DETAILS

Gimel combines open-source
with proprietary services

Gimel Technologies

➤ Focus: Monetization

Gimel Foundation

➤ Focus: Adoption

TRANSPARENCY · *Basic functionality must not be a “black box”*

4. INVESTMENT DETAILS

Three Target Groups – three key Use Cases



CISO

Chief Information Security Officer

Protects against deepfakes through DNA-precise identity verification and implements post-quantum cryptography for critical systems.



CIO

Chief Information Officer

Scales AI teams with verified human-machine coordination and AI Agent Protocols for secure agent orchestration.



COO

Operations Leadership

Ensures security for Digital Agents and Robots through verified command chains and resolves liability issues with auditable logs of actions.

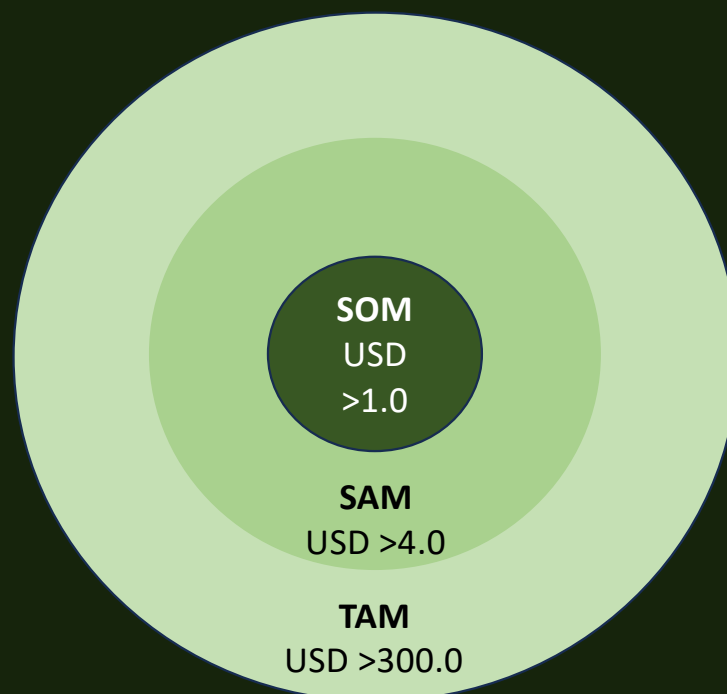
4. INVESTMENT DETAILS

AI Foundation for Control and Quantum Resistance: A Market with Massive Potential

Total Addressable Market

Software and Hardware for Artificial Intelligence solutions globally

Volume: USD >300,0 bn.
CAGR: >25 percent p.a.



Serviceable Available Market

AI Governance and Security solutions for Agentic and Physical AI, including AGT, PaC and IAM solutions

Volume : USD >4.0 bn.
CAGR: >35 percent p.a.

Serviceable Obtainable Market

Next-level AI Governance and Security solutions in line with regulations like EU AI Act amongst others (e.g., LoA5)

Volume : USD >1.0 bn.
CAGR: >50 percent p.a.

Sources: Gartner, Forester, IDC

Basis: 2026

AGT: Microsoft AI Governance Toolkit; PaC: Policy as Code; IAM: Identity and Access Management (e.g., Microsoft Entra Agent ID)

4. INVESTMENT DETAILS

Our Business Model and Go-to-Market Strategy

Our Market: The Serviceable Obtainable Market for Gimel is growing at an annual rate of >50% (CAGR).

Our Model: GIMEL offers a highly scalable AI Foundation Layer facilitating AI Control and Quantum Resistance.

Our Strategy: Focus on Critical Infrastructure, globally, Government Agencies in Europe, Corporates and SMEs.

Open Core: Transparency through open-source protocols paired with proprietary services (“Gimel Moat”)

Different sources of income ensure sustainable growth and scalable margins for both our AI Control and Trust Infra solution:

One-time / Monthly Fee

Charge per human user (Gimel ID) or governed Agent (Gimel Auth).

Monthly fee for verified identities and/or AI agents with a complete audit trail.

Transactions Fee

Per verified action (e.g., per token refresh for Gimel ID / PQC, agent request for Gimel Auth, etc.).

A small fee per verified action that increases with volume.

Conformance Testing

Quality Assurance of Gimel solutions in the Partner Network.

Further improvement of proprietary AI solutions, incl. threat-patterns update and federated learning.

4. INVESTMENT DETAILS

Gimel shareholdings are structured in line with funding and team retention targets

Shareholder	Percent	Role	Basis
Daniel Hartert	3.5	Chairman of the Board	Shareholders Agreement
Dr. Francesco De Meo	3.5	Board Member	
Dr. Götz Wehberg	63	Co-CEO	
Team	30	Core Team	VSOP
Investors	Prospectively	Strategic / financial investor	Term Sheet

From Series-A onwards, **Gimel Holding** will be set up as investment vehicle and AssetCo, hosting Gimel Technologies as OpsCo, etc.

4. INVESTMENT DETAILS

Traction data points

*Non-dilutive
funding of USD
1 million**

*>4 PCT-patents
pending for
all services*

*PoC-customers
being launched
(incl. 3 SI-providers)*

*GA-intend by
Top-3 DAX
company*

*Certified Lab-infrastructure
at German University
Clinics*

*Supported by
globally leading
cyber center***

*160 agents
represented in
Foundry*

*1,300
occupancies
in GAuth*

*60,000
precedents
trained*

*Team with
>200 years
accumulated*

GA: General availability (Github status)

* By German Ministry of Research, Technology and Space

** By Helmholtz Center for Information Security

Note: Series-A and B in planning stage

4. INVESTMENT DETAILS

Gimel currently onboards seed investors

	Seed	Series-A	Series-B
Focus	Acceleration of Product Development	Scalability	Growth & Product Expansion (Gimel ROS, etc.)
Time	12 – 24 months	Ca. 1 -2 years after Seed	Ca. 2 – 3 years after Series-A
Investment Form	Convertible Loan	Equity	Equity
Targeted ARR	USD 7 Mio.	USD 80 Mio.	USD 300 Mio.
Targeted EBITDA	USD -3 Mio.	USD +/- 0 Mio.	USD 50 Mio.
Investment Need	USD 5 Mio.	USD 60 Mio.	USD 300 Mio.

Note: Series-A and B in planning stage

CONTACT

Gimel Technologies

Hardtweg 31
53639 Königswinter, Germany

Bjørn Baunbæk and Dr. Götz Wehberg, Managing Director

Tel.: +4915112462890

Mail: gwehberg@GimelID.com

Web: <https://gimel.io>

Github: <https://github.com/Gimel-Foundation>

See investor video:



Legal notice: All rights are reserved. The brands and concepts of Gimel Technologies GmbH and its affiliated companies are protected by copyright. The products, procedures and services of Gimel Technologies GmbH and its affiliated companies are protected by patent law (patents pending).

This presentation contains forward-looking statements that involve substantial risks and uncertainties. All statements other than statements of historical fact could be deemed forward-looking, including statements regarding market opportunity, projected financial performance, growth rates, and strategic plans. These statements involve known and unknown risks, uncertainties, and other factors that may cause actual results, performance, or achievements to differ materially from those expressed or implied by the forward-looking statements. Factors that could cause such differences include, but are not limited to: market competition, regulatory changes, technology development delays, customer adoption rates, operational challenges, and general economic conditions.

Investment in early-stage technology companies involves a high degree of risk. Investors should be prepared for the possibility of losing their entire investment. Past performance is not indicative of future results. The projections and estimates contained in this presentation are based on management's current expectations and assumptions and may not be achieved. Market conditions, competitive dynamics, and regulatory environments may change in ways that adversely affect the company's business and financial performance.

