

Enterprise Shadow Cryptography

Why visibility matters now more than ever

Yannik Goldgräbe
Swiss Cyber Storm 2026





Yannik Goldgräbe

- Security Architect, B2B Application Security
- Expert for Applied Cryptography & Protocols
- Member of Swisscom PQ Core Team



E-Mail: yannik.goldgraebe@swisscom.com
LinkedIn: <https://www.linkedin.com/in/yannikgold/>



Overview

1. Shadow Cryptography Definition
2. Enterprise Example (IAM)
→ Zoom-in & Zoom-out
3. Four Catalyzing Storms
4. Tackling the Challenge
5. Compact Playbook



Shadow cryptography: the cryptography you rely on but can't see, inventory or govern end to end.





Enterprise Example

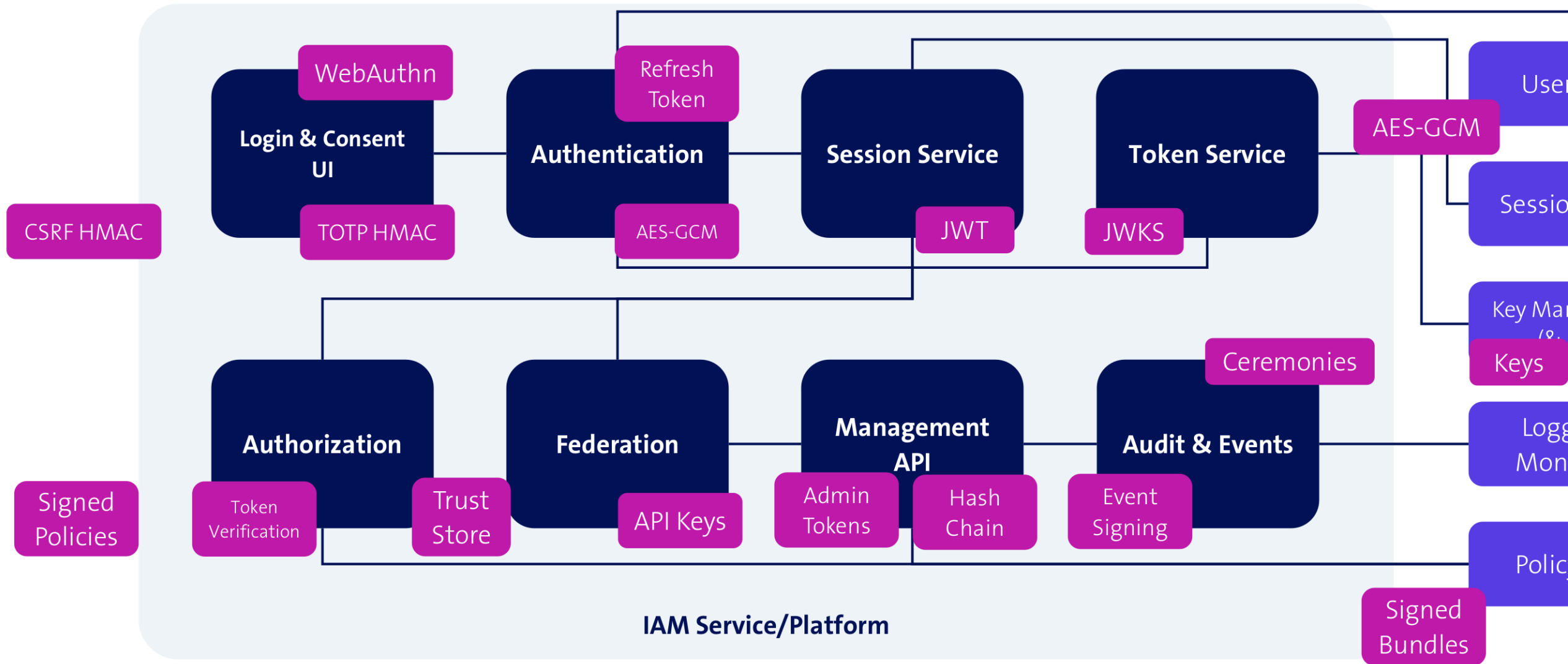
Generic



IAM = **Identity & Access Management**, a common service found in enterprise environments



IAM Example *Architectural Zoom-In*

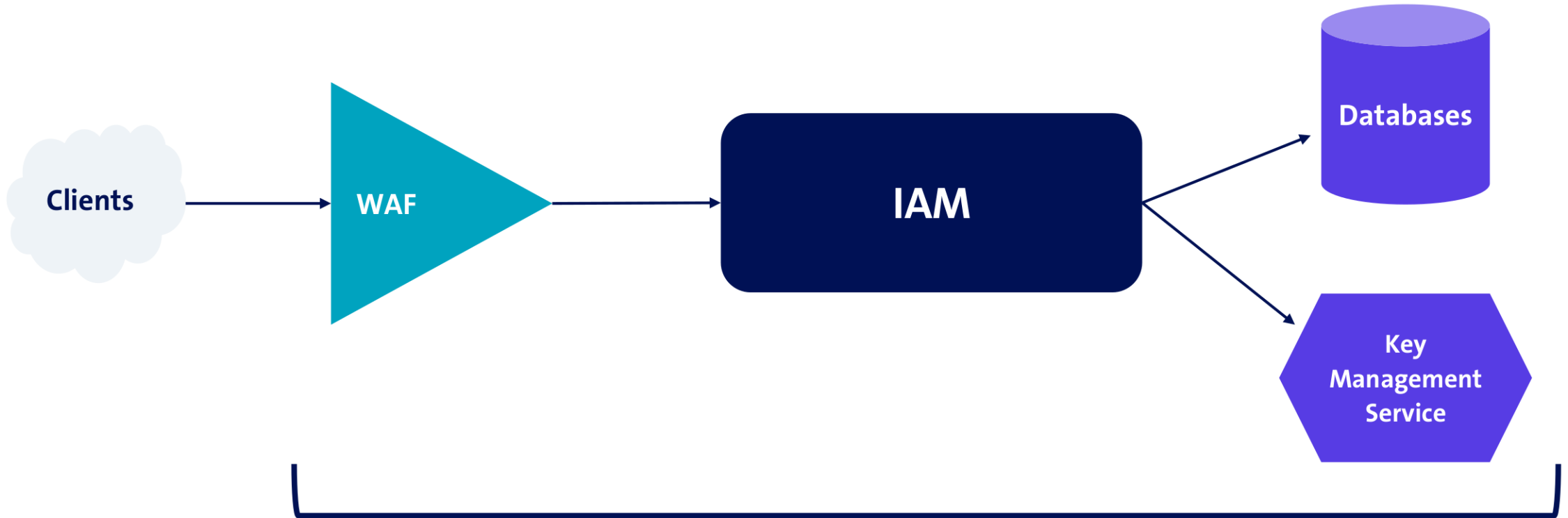




IAM Example

Zoom-out

Software Cycle
Artifact Signing, Workload Attestation, etc.





« Healthy **cryptography** is everywhere and invisible, because it works.

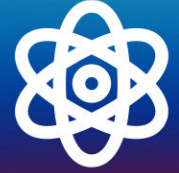
It's not weak per se, but **it's mostly unmanaged**, which creates future risks.



Regulation



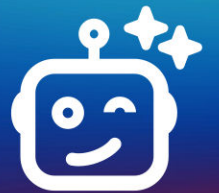
Quantum



Certificate
Lifetime



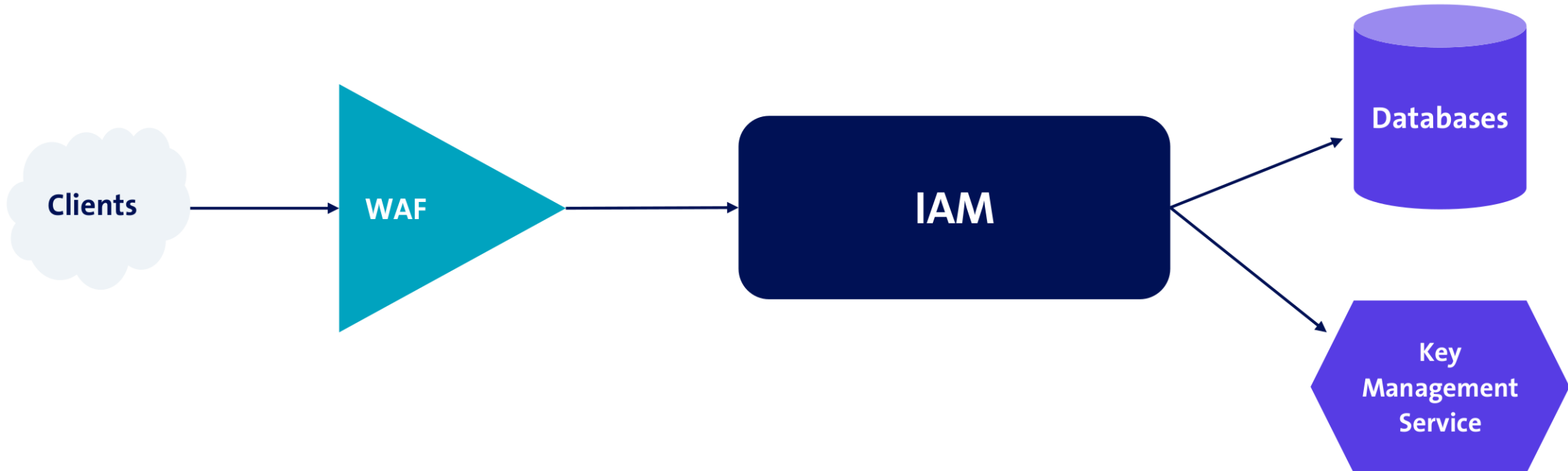
AI





IAM Example

Zoom-out





IAM Example

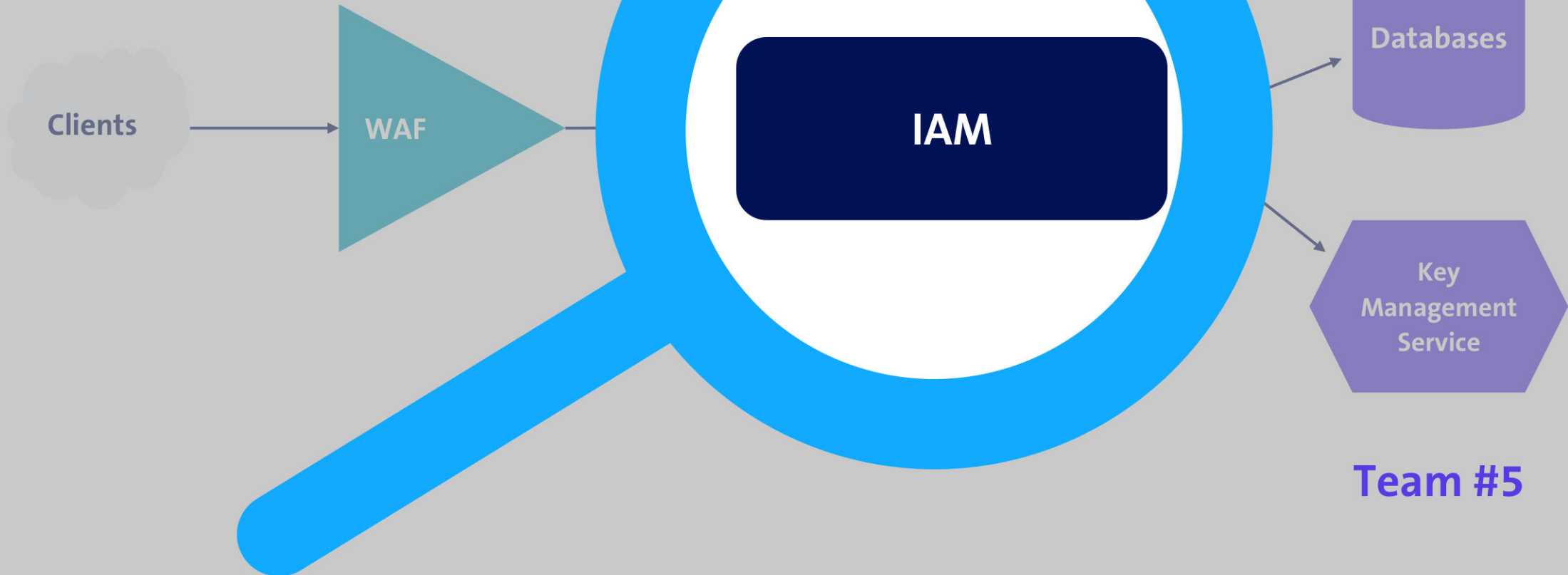
Shadowy

Team #3

Team #4

Team #2

Team #1





Tackling the challenge...

So, what to do?



Cryptographic Inventory

Concept Introduction

What is it?

A living record of every cryptographic asset: algorithms, keys, certificates, protocols, libraries, hardware incl. owners and dependencies.

Layers of scope and depth

- **Network:** endpoints, certificates, TLS configurations (what scanners see)
- **Software:** libraries, algorithms, key usage in code and pipelines
- **Host:** OS crypto providers, kernel and runtime stacks, disk and volume encryption, local key stores
- **Hardware:** HSMs, TPMs, secure enclaves and their firmware



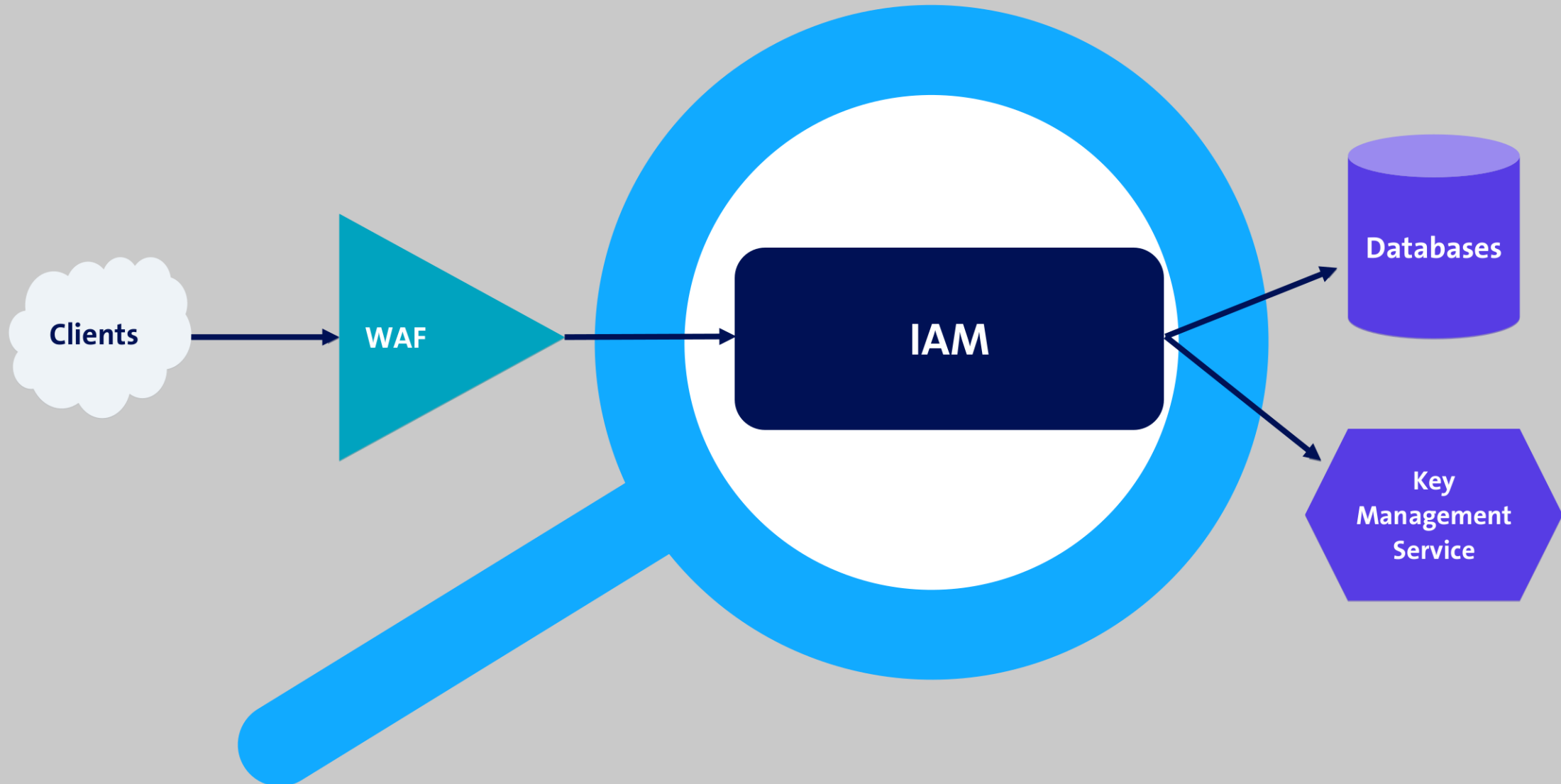
What it's for?

1. **Visibility:** know what exists and who owns it
2. **Prioritization:** rank by data lifetime, exposure and algorithm risk
3. **Migration Planning:** turn the inventory into the backlog
4. **Governance & Control:** policy enforcement, drift detection, agility enablement



IAM Example

Adding light to the shadow





Shadow Cryptography Playbook

A high-level cheat sheet

Discover & Trace: Light what you can reach, follow the handshake(s)

Own: Assign the flow, not the box. One accountable owner per data flow.

Modernize, triage by data lifetime

- Focus: long-lived confidential data and legacy algorithms
- First: external and public-facing interfaces
- Last: short-lived internal traffic

Automate, prepare for **Agility**

- Keys only via KMS/HSM APIs, rotation as code
- Cryptography behind an abstraction layer, so algorithms can be swapped without a rewrite

Establish a small CCoE (Cryptographic Center of Excellence)

2–3 people beat a large program: they set the policies, review the flows and preserve the integrity of the inventory



Thank you!

E-Mail: yannik.goldgraebe@swisscom.com
LinkedIn: <https://www.linkedin.com/in/yannikgold/>