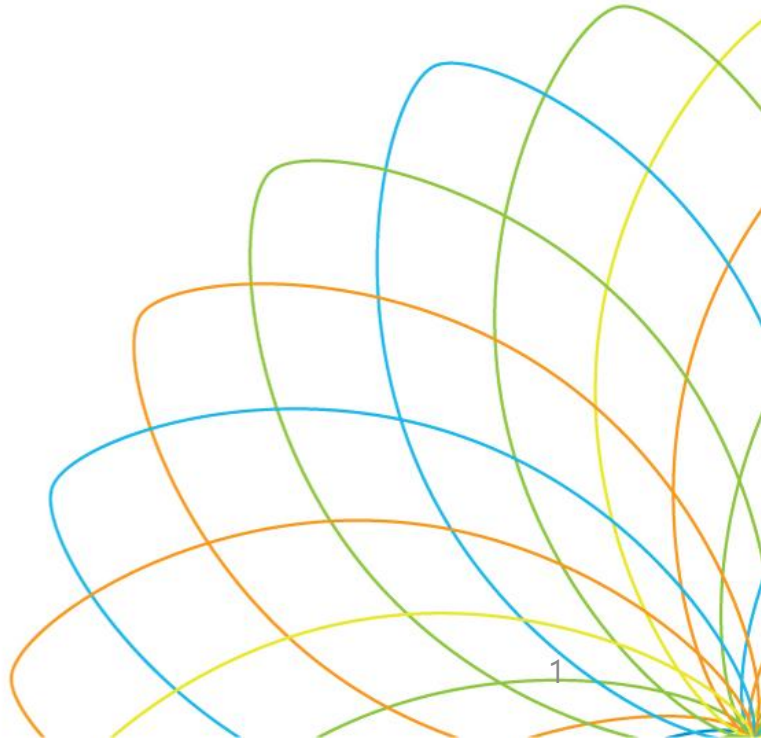
Agentic AI Management using PKI(LDAP)

ChangGyun Kim

DSMentoring Co, Ltd



Contents

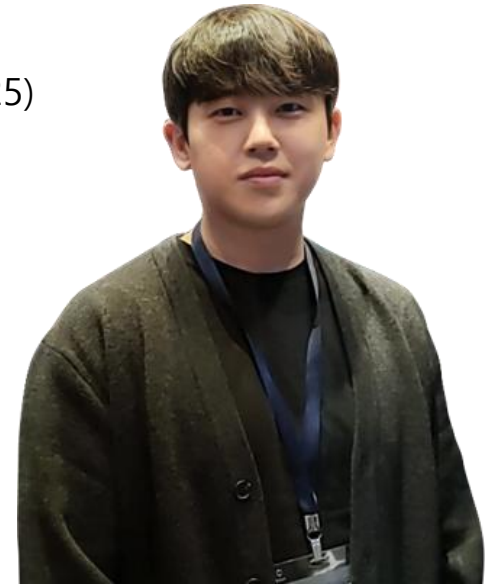
Introduction

Who Am I

ChangGyun Kim

- Education
  - ❖ Imperial College London MSc Computing (~2022), with a focus on Artificial Intelligence

- Career
  - ❖ SANDS Lab Inc. (2023~2026)
    - File Lineage Analysis through Function Similarity Tracking (Presented in Virus Bulletin 2023, 2025)
    - Cybersecurity RAG-based sLLM Development and Demo Platform Implementation (~2026)
  - ❖ DSMentoring Co., Ltd. (2026~)
    - Building AI Agent-based Workflow Automation

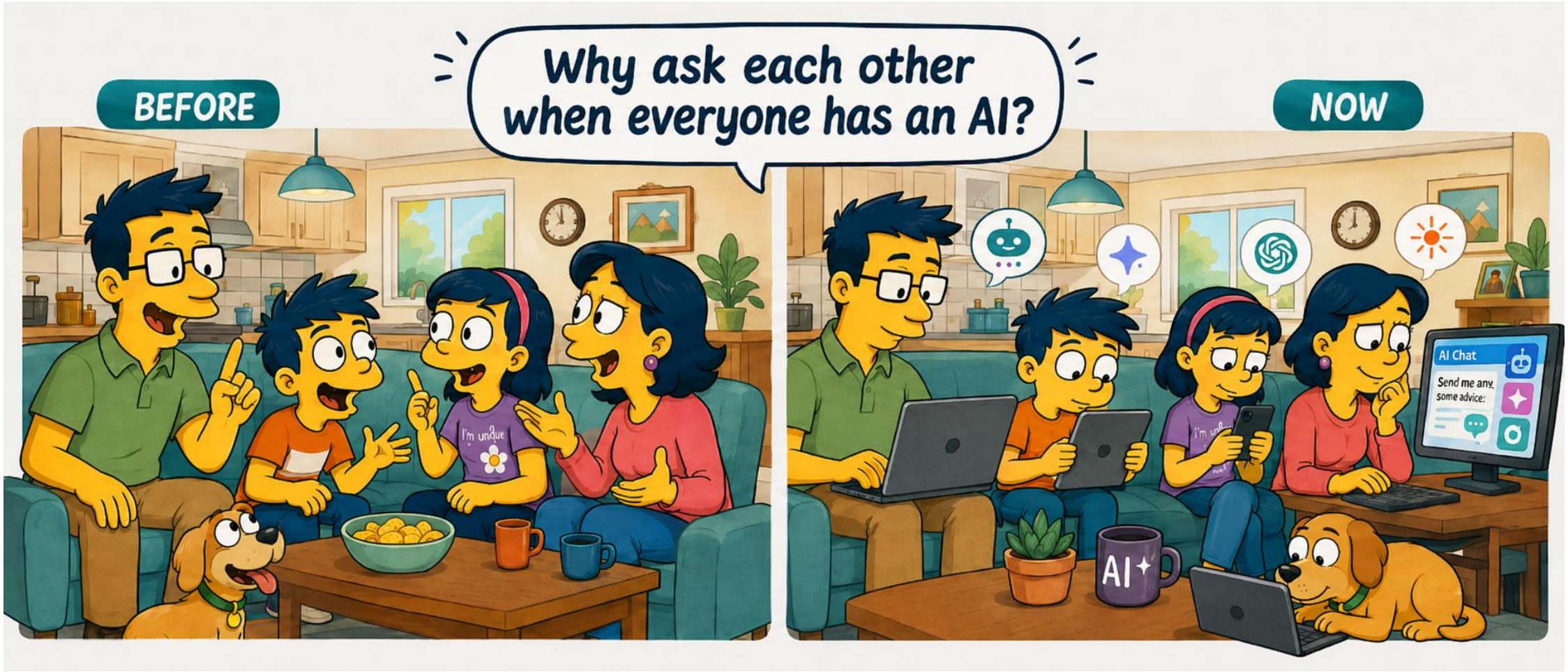


Problem Statement:
Why Agentic AI Should Be Treated as NHI

- **So Many AIs, So Many Agents**
- **From ChatBots to Non-Human Actors**
- **The Question Has Changed**

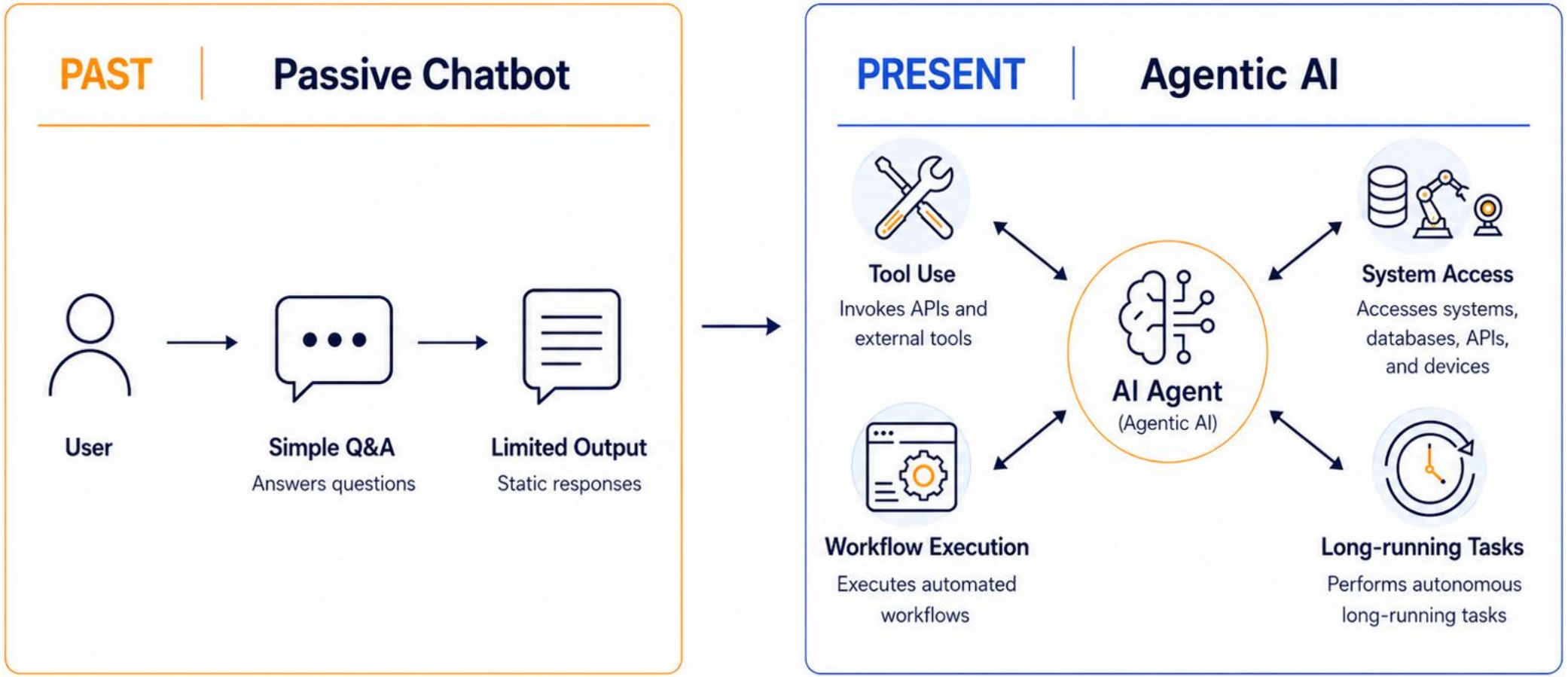
So Many AIs, So Many Agents

- **AI services are everywhere!**



From Chat-bots to Non-Human Actors

- Agentic AI is no longer a passive assistant.
  It operates as a **Non-Human Actor inside Digital and Physical Systems**.



Agentic AI should be managed as a **Non-Human Identity (NHI)**.

The Question Has Changed

The Key Question shifts from **"Who is it?"** **to** **"What can it do?"**

Human IAM

- "Who is this account?"

- Account Management
  - ❖ Authentication
  - ❖ Account Identity
  - ❖ Login Session
  - ❖ Role Assignment

Agentic AI IAM

- "What is this agent allowed to do?"

- Privilege-use Management
  - ❖ Tool Invocation
  - ❖ Data Access
  - ❖ System Operation
  - ❖ Physical or Logical Action

From an **Account model** to an **Action-permission model**

A New Perspective: From Identity to Capability

- **Decoupling: PKI vs PMI**
- **Attribute Certificate for NHI**

Decoupling: PKI vs PMI

Pillar 1: PKI

- Mechanism
  - Public Key Certificate (PKC)
- Core Question
  - "Who is this?"
- Primary Purpose
  - Authentication
- Lifespan
  - Long-lived Identity

Pillar 2: PMI

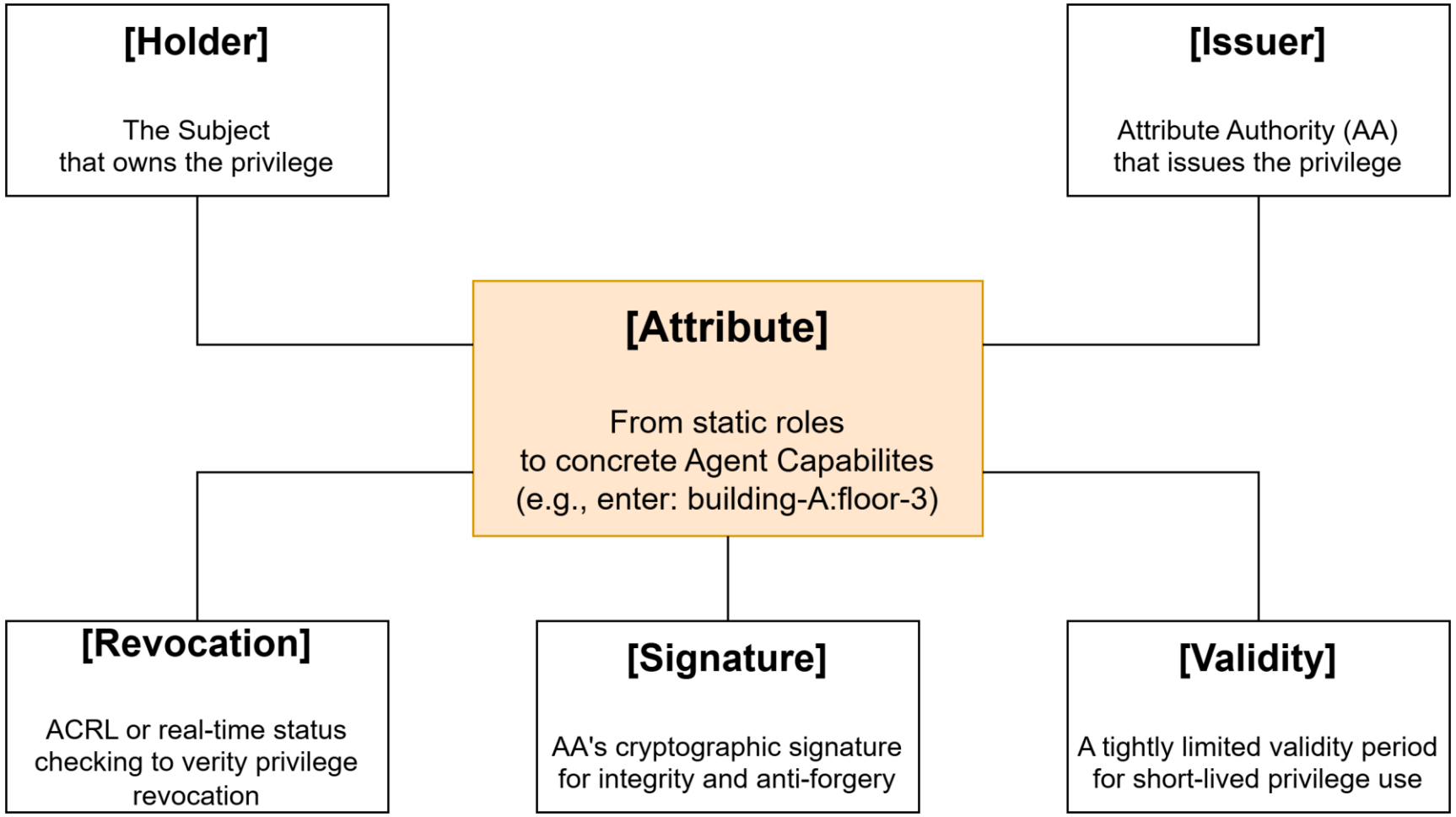
- Mechanism
  - Attribute Certificate (AC)
- Core Question
  - "What can this do?"
- Primary Purpose
  - Authorization
- Lifespan
  - Short-lived Capability

Benefits of Separation

1. Modify capabilities without re-issuing identity.
2. Revoke privileges instantly without terminating the underlying identity.

Attribute Certificate for NHI (AI Agents)

- **An Attribute Certificate is a standalone privilege object that carries the agent's concrete capabilities**



Management Model: Classification, Requirements, and Structure

- **Not All NHIs Are the Same: Three Classes of NHI**
- **Design Requirements: R1-R5 for NHI Capability Management**
- **Extended LDAP DIT: For NHI Privilege Management**

Not All NHIs Are the Same: Three Classes of NHI

Not all Non-Human Identities require the same Authorization Infrastructure

- The LDAP-based model supports all three NHI classes
  - using customized configurations for each class and risk level

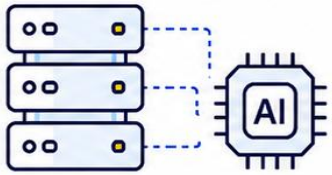
Class A
Persistent Physical NHI

Examples
Humanoid robots, OT systems, IIoT devices

Why it fits
- Direct connection to physical safety
- Strong need for geofencing and safety tiers
- Clear owner-operator relationship required

Primary Target

Class B
Persistent Virtual NHI



Examples
Long-running AI agents, automation bots, service accounts

Why it fits
- Sustained capability ownership
- Need for precise privilege control
- X.509 AC serves as capability attestation layer on top of OAuth/OIDC

Major Target

Class C
Ephemeral Virtual NHI

Examples
Task-level LLM agents, ephemeral containers, short-lived execution instances

How it fits
- TTL-based auto-expiry supports short-lived identities
- Low-risk access credentials can use longer cache duration
- Emergency group-wide revocation is available when needed

Adaptive Fit

Design Requirements: R1-R5 for NHI Capability Management

Five requirements define what the LDAP-based NHI model must satisfy
And how each shapes the DIT structure

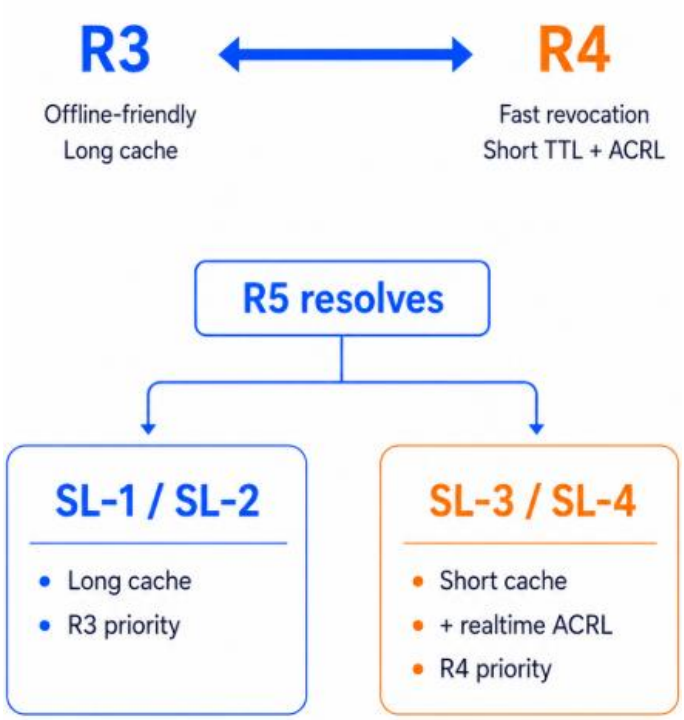
The Five Design Requirements

The Five Design Requirements

#	Requirement	Core Question	Resolved By
R1	Fine-grained Capability Expression	Actions, not roles?	Hierarchical capability namespace in ou=AC
R2	Identity–Privilege Separation	PKC and AC lifecycle independent?	ou=NHI (identity) vs ou=AC (privilege)
R3	Intermittent Connectivity	Operate without constant server access?	TTL-based cache + Dynamic Entry
R4	Fast Revocation	Revoke instantly when needed?	ou=ACRL + Delta-ACRL + KillSwitch
R5	Trust Tiering	Different assurance per risk level?	Tier-1/2/3 + SL-1 through SL-4

Tier-1/2/3: maximum trust tier
SL-1~4: maximum safety level

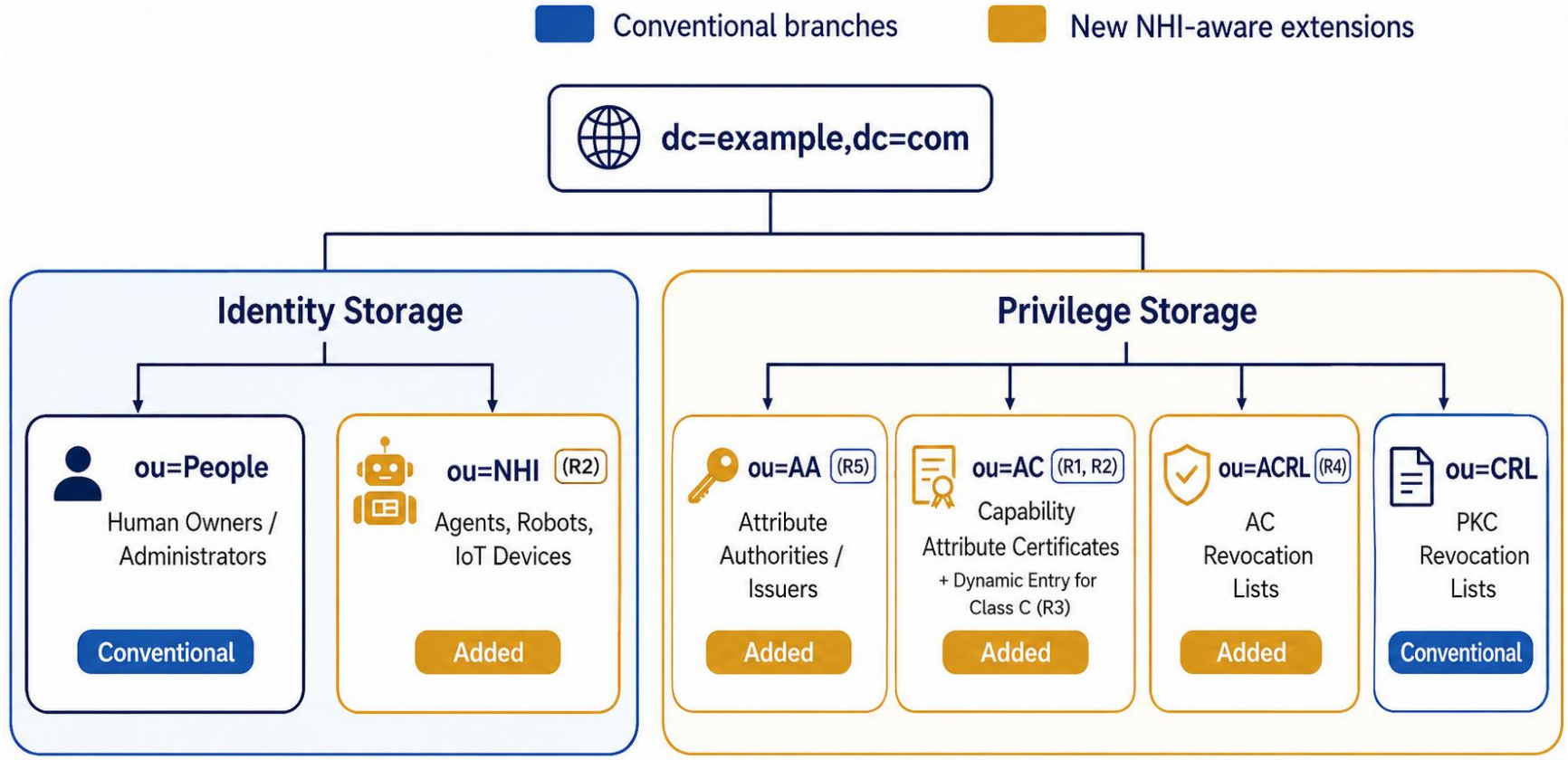
R3 vs R4



Extended LDAP DIT: For NHI Privilege Management

Extended DIT

1. ou=NHI separates Non-Human identity from privilege objects (R2)
2. ou=AA with Owner-as-AA enables distributed capability issuance (R5)
3. ou=AC carries fine-grained capability namespace per NHI (R1, R2)
4. ou=ACRL with Delta-ACRL and KillSwitch enables fast revocation (R4)



Standardization and Verification Architecture

- Need for NHI-aware Standard Extensions
- Capability Verification Model Pipeline

Need for NHI-aware Standard Extensions

- **Existing IETF standards provide structural foundations**
  - But not NHI and Privilege Awareness
  - RFC 4523 standardizes LDAP for PKI storages, while RFC 5755 defines a general Attribute Certificate profile
  - However, both still leave important gaps for NHI privilege management

RFC 4523
LDAP X.509 PKI Schema

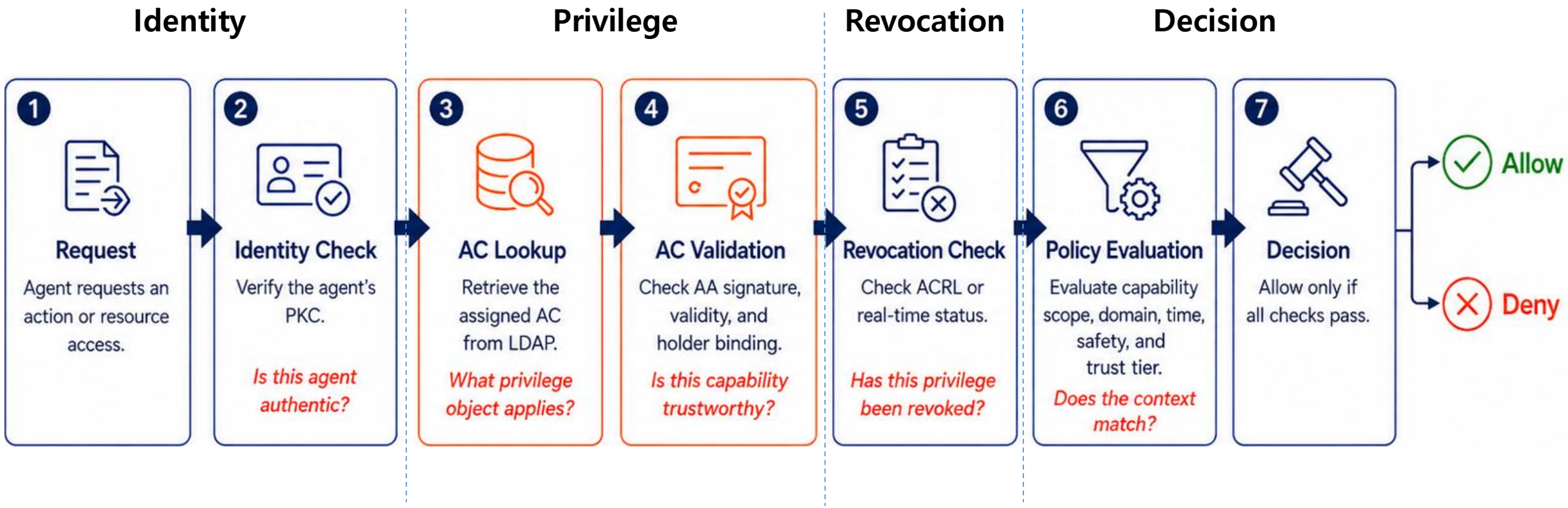
Provides	• LDAP schema for PKI objects • Certificate and CRL storage • Basic X.509 directory profile
Still Missing	• AC / ACRL storage profile • NHI-aware entity structure • Capability-oriented directory organization

RFC 5755
Internet Attribute Certificate Profile

Provides	• General AC structure • Basic validation model • Internet AC profile
Still Missing	• NHI capability semantics • Operational domain / geofencing • Owner delegation semantics • Safety level representation • Emergency kill-switch meaning

Capability Verification Model Pipeline

LDAP-based Capability Verification Flow



Architectural Principle: **Default-Deny, Whitelist-based Capability Authorization**

Conclusion

Conclusion

Agentic AI (NHIs) management is not only an Identity Problem
It is a Privilege Attestation Problem

- **Identity is Not Enough**
  - PKI alone cannot secure Physical, High-Risk, and Complex Digital Agentic Actions

- **Rebirth of the AC**
  - The X.509 Attribute Certificate, reinterpreted as an Agent Capability Object, supports all three NHI classes – from physical robots to ephemeral agents

- **The LDAP Substrate**
  - LDAP provides the Structured Management Layer – separating Identity (ou=NHI) from Privilege (ou=AC, ou=ACRL) and enabling R1-R5 by design

- **Standardization Direction**
  - Extending RFC 4523 and RFC 5755 would provide a clearer basis for NHI-aware Privilege Management