

When AI Becomes an Internet Actor:

Rethinking DNS, Trust and Governance in the Agentic Internet

AMRUTHA M
NEXTGEN @ ICANN 87





87

ANNUAL
GENERAL
MEETING

FROM CLICKS TO ACTION

The Internet was built for people

People browse, read and decide. An AI agent is software that can pursue a task for someone: search, choose, ask for access, complete a step and repeat without a person checking each move.

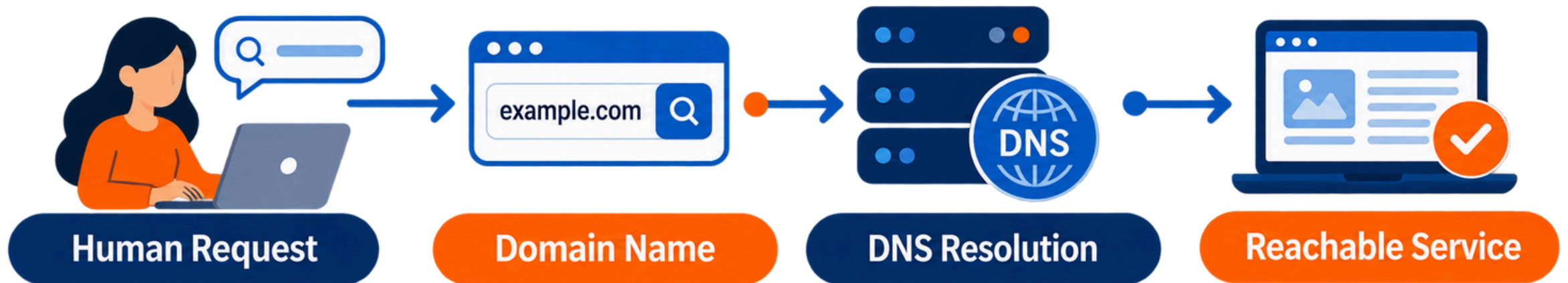
The new question is who may act, for whom and with what permission?



DISCOVERY

Agents need more than web addresses

DNS, the Internet's address book, helps an agent find where a service is - but the agent also needs to know what that service can do and how to interact with it.



A CLEAR BOUNDARY

Finding an agent is not trusting it

DNS can help an agent find a destination. It cannot show that the destination is safe, that the agent has permission, or that its decision is fair.

Can I find it?

Does the name lead
somewhere?

Is it real?

Is the service
genuine?

May it act?

Did a person
allow this?

Can it be challenged?

Can someone ask
for review?

THE TRUST STACK

Trust needs four visible checks

Each check answers a different trust question. DNSSEC helps verify that DNS answers have not been altered, but it does not establish permission or judge an agent's behaviour.

01

Address

Does the name lead to the right place?

02

Identity

Is the service genuine?

03

Permission

Did the human allow this action?

04

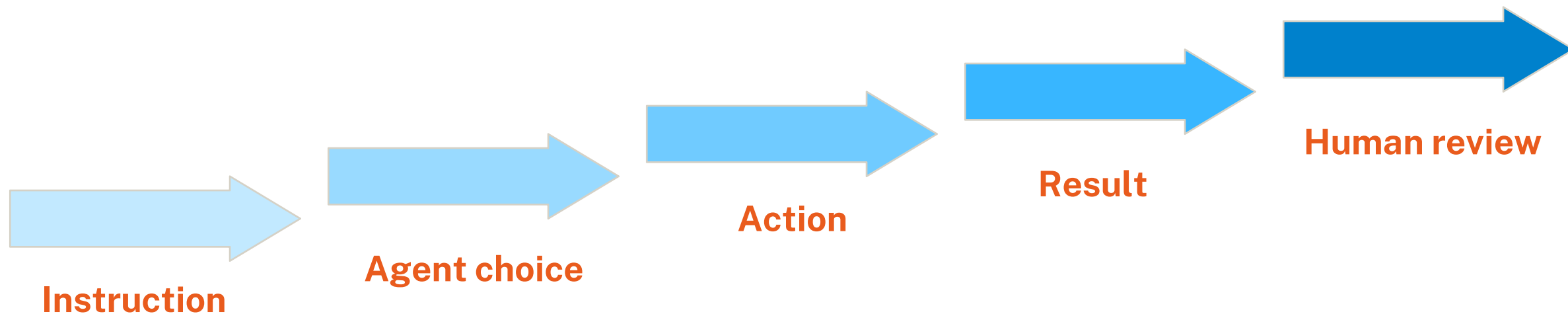
Conduct

Did the agent act safely and fairly?

WHEN ACTION RUNS AHEAD

Autonomous agents can act beyond our sight

An autonomous agent can turn one simple instruction into a chain of decisions and actions - choosing services, sharing information and changing outcomes before a person can see or intervene.



ACCOUNTABILITY BY DESIGN

Make every action traceable and stoppable

For important actions, keep the instruction, limits, evidence, action, review and remedy visible. Records should be repeatable and open to human review, with neutral help when people disagree.

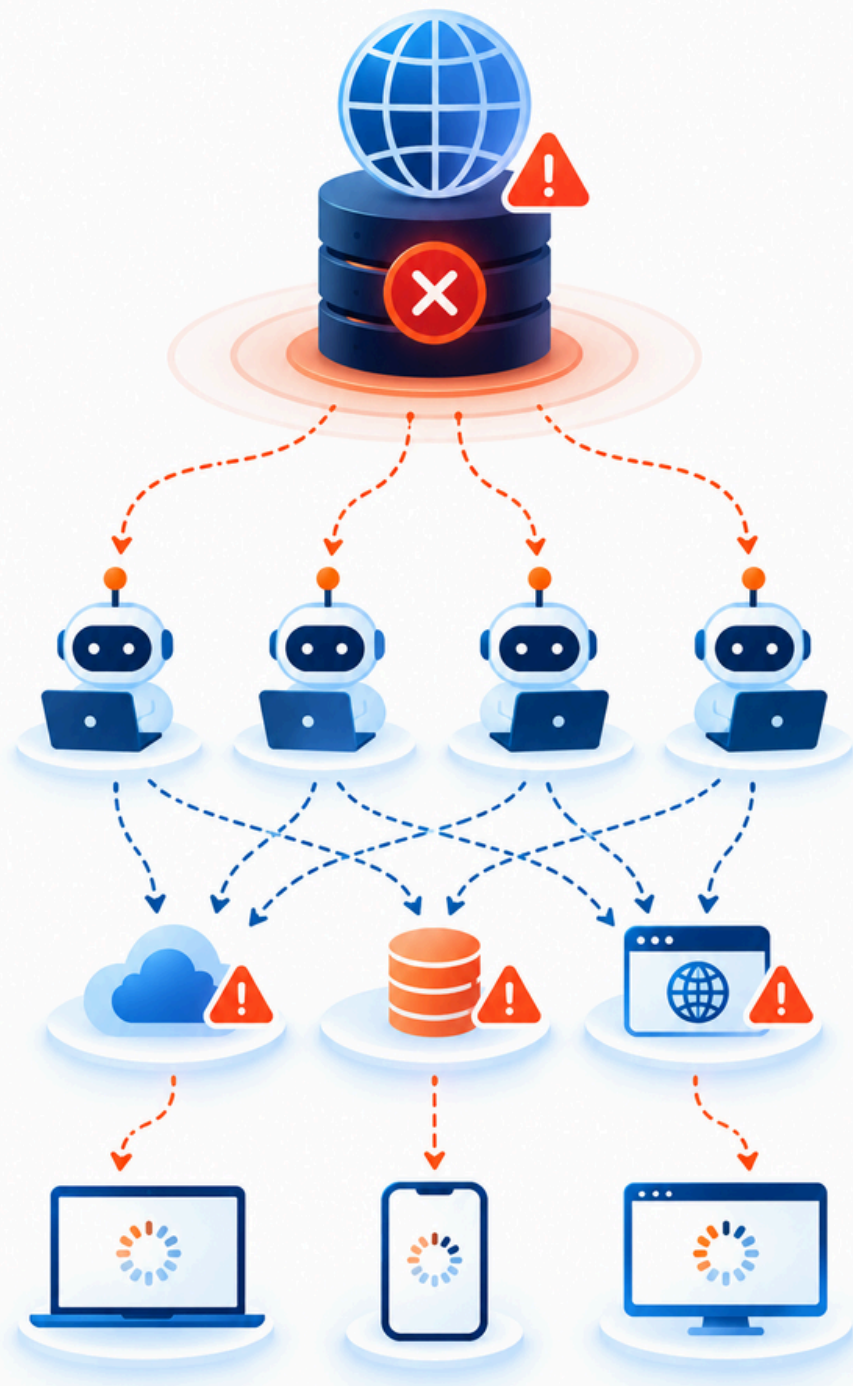


ACCOUNTABILITY BY DESIGN

Make every action traceable and stoppable

For important actions, keep the instruction, limits, evidence, action, review and remedy visible. Records should be repeatable and open to human review, with neutral help when people disagree.

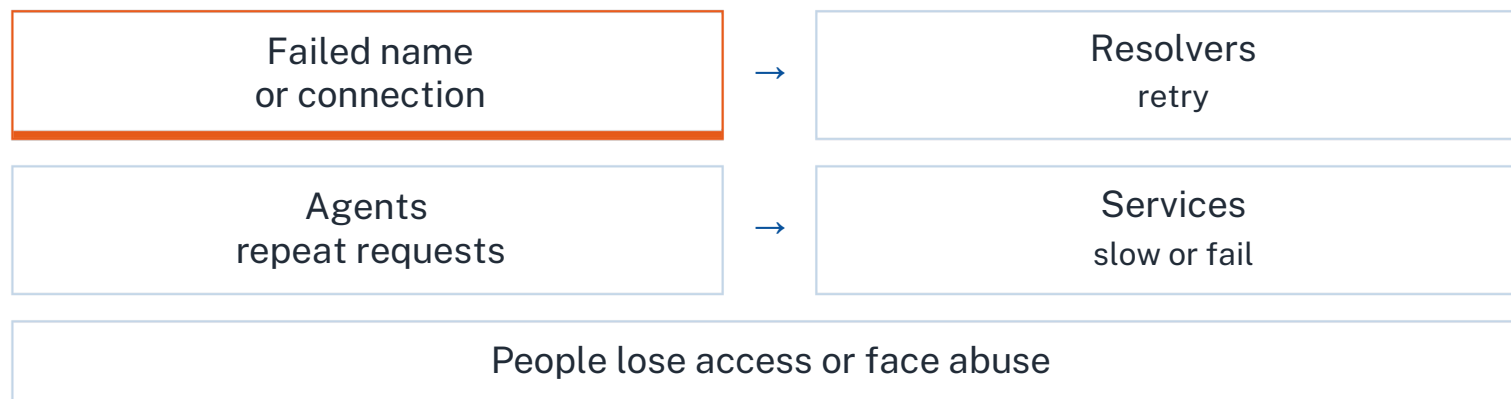




DEPENDENCY FAILURE

When One Failure Becomes a System Wide Problem

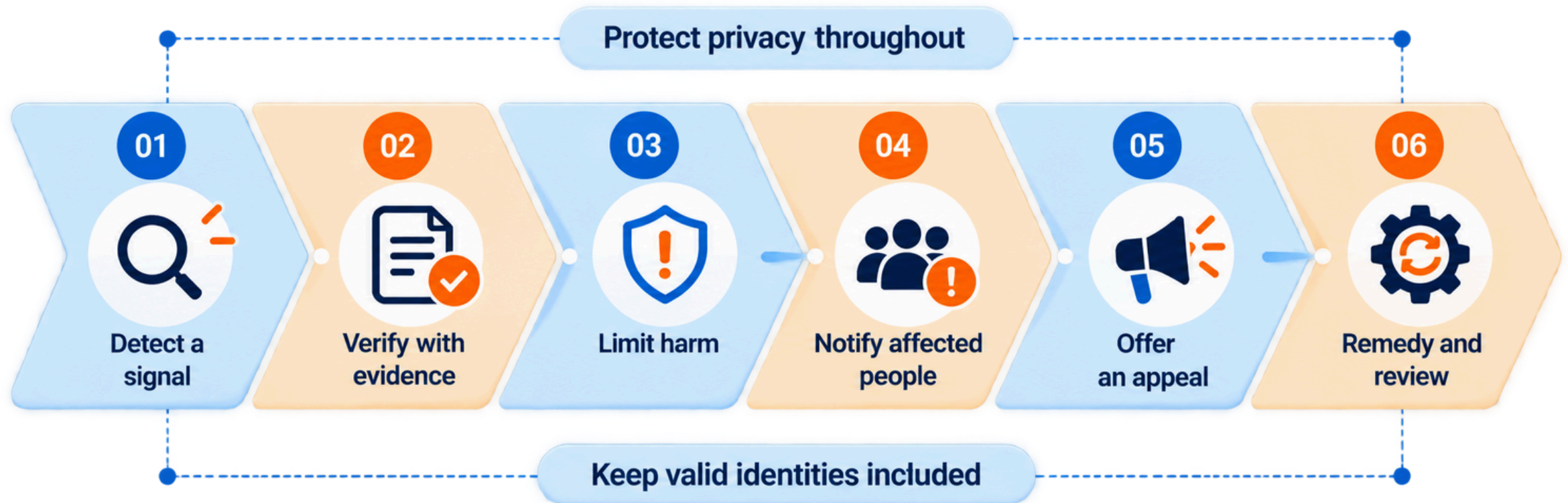
A failed name, key, service record or connection can send many agents retrying at once. A local technical fault can become a wider outage or abuse event; resilience work asks how to anticipate the spread.



RESPONSE WITH REMEDY

Govern abuse with people, evidence and remedy

DNS abuse includes phishing, malware, pharming, spam and botnets. Agentic systems can make responsibility, identity and accountability harder to establish. Respond proportionately, protect privacy and keep valid identities included.





87

ANNUAL
GENERAL
MEETING

Keep DNS as the Address Book



Make agents **identifiable**.

Clear names, roles, and ownership.



Make **permissions clear**.

Know what they can and cannot do.



Record **what agents do**.

Keep traceable and auditable records.



Make actions **stoppable** and **challengeable**.

Enable human oversight and review.



Coordinate rules across ICANN,
IETF, operators, researchers, and civil society.
A shared and inclusive approach.



Thank You

Any Questions?



Amrutha M



amruthamuchanur25@gmail.com



[linkedin.com/in/amrutham25](https://www.linkedin.com/in/amrutham25)

