WE ARE DEVELOPERS · BERLIN · 9/10 JULY 2026

Beyond authentication: an open source trust model for the agentic web

Sabrina Engling
AI Lead
Trusted Shops

Alexander Günsche
Senior Solutions Architect
Amazon Web Services

Traditional e-commerce

User

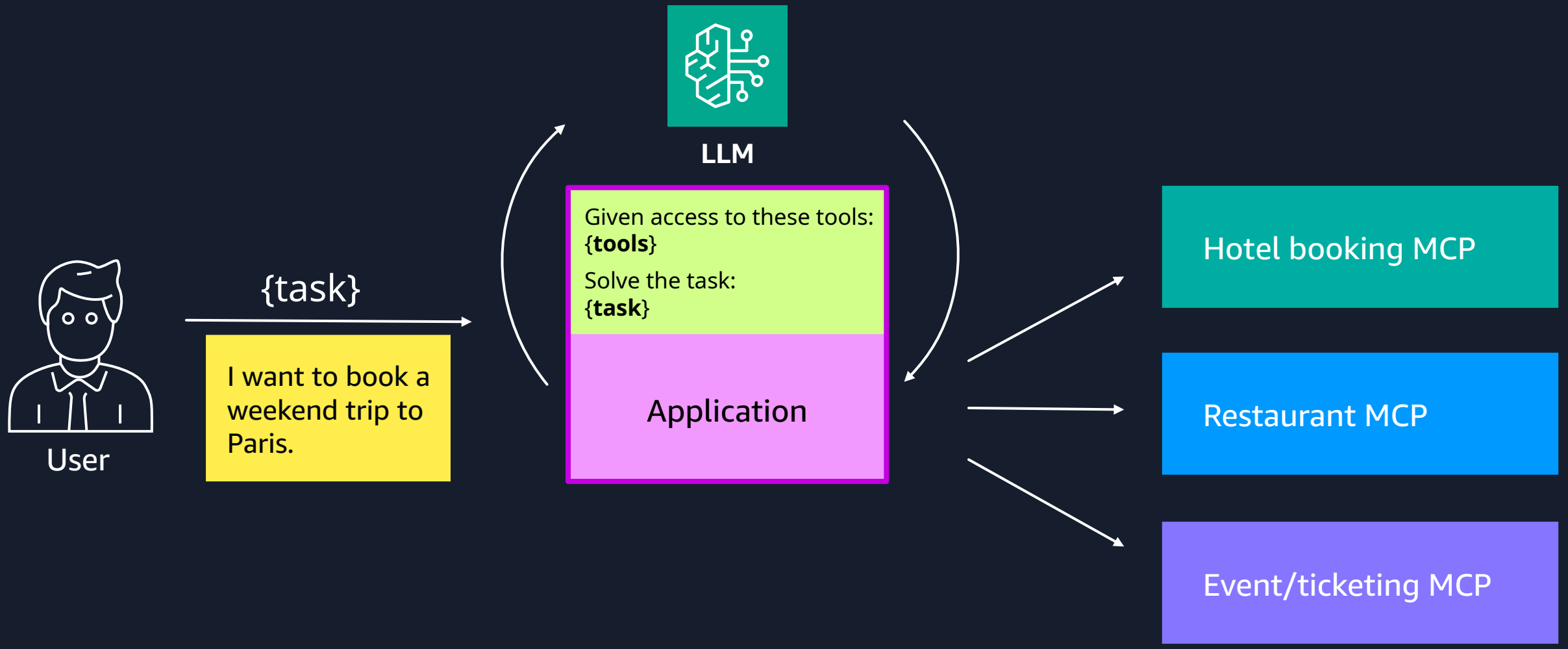
I want to book a weekend trip to Paris.

Hotel booking site

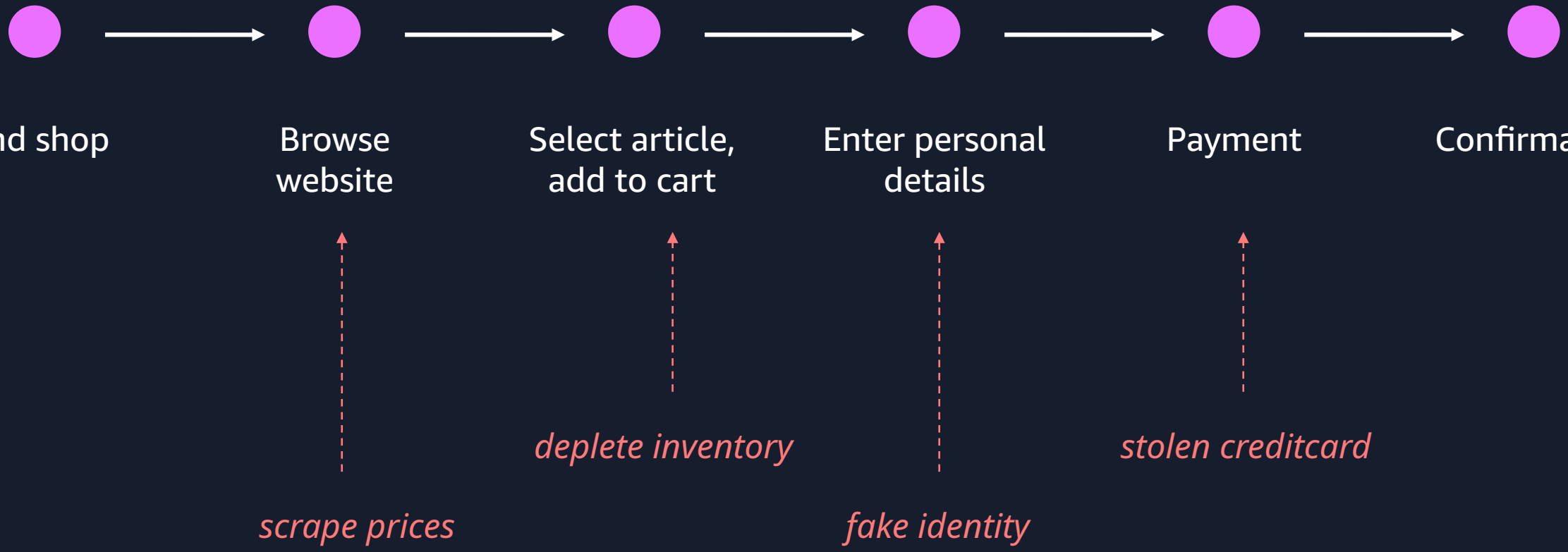
Restaurant site

Event/ticketing site

Agentic e-commerce



Do you trust your “customers”?



The problem is already there

Automation captures scarce inventory, redirects value and damages customer trust.

Concert tickets

Eras Tour sale

Observation

3.5B system requests overwhelmed Ticketmaster.

Business impact

Fans lose access; value moves to resale markets.

Sneaker drops

Nike SNKRS

Observation

Up to 12B bot calls per month; hot drops can see 10–50% bot entries.

Business impact

Launch hype turns into frustration for real customers.

Hardware launches

Consoles, GPUs, controllers

Observation

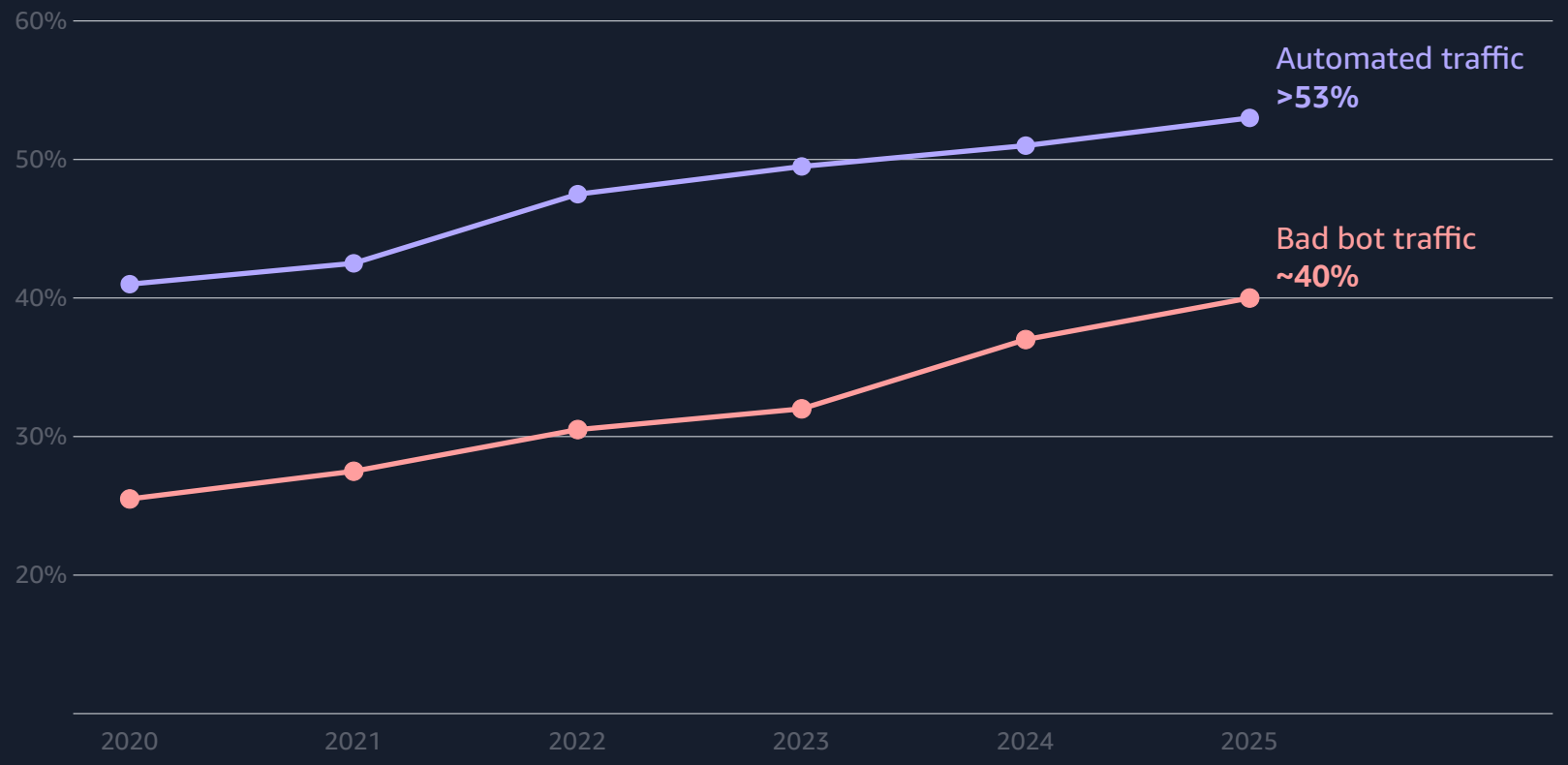
Scarce products sell out quickly and reappear at multiples of retail price.

Business impact

Brands lose control over price perception and customer experience.

Automated traffic

Bots are significant portion of web traffic, with malvolent traffic a major share.



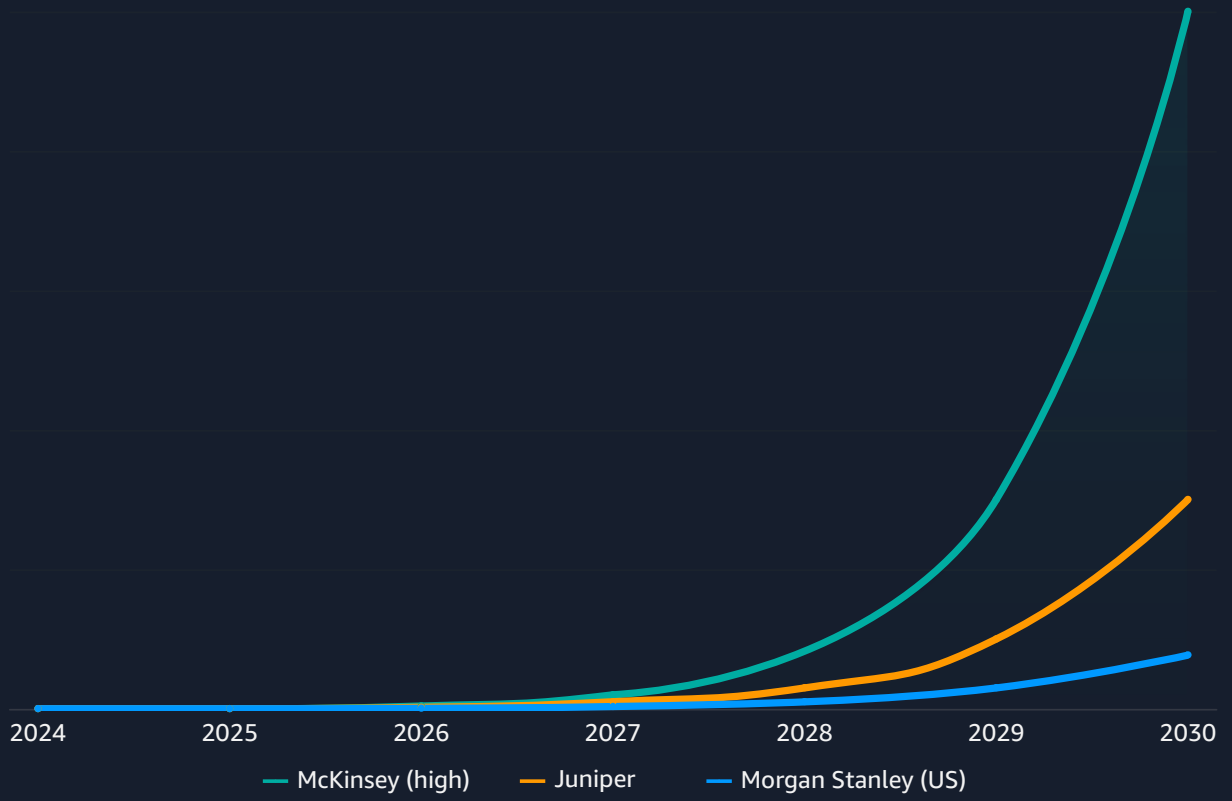
Sources: Imperva/Thales Bad Bot Reports 2021–2026; values rounded from public summaries.

Evolution of the agentic landscape

Over the next few years, agentic traffic will grow from a small share to a dominant portion of digital traffic.

Service providers can't tell legitimate agents from malicious bots. Every automated request looks the same.

Agent operators can't prove their agents are trustworthy. They fight an arms race to retain access.



Agentic use cases: More than e-commerce

PERSONAL & PRODUCTIVITY

- Personal travel concierge
- Inbox autopilot
- Tax returns, prepared and filed
- Insurance claim advocate

KNOWLEDGE WORK

- Overnight investment research
- Legacy code migration
- Self-driving research labs
- Due-diligence document review

ENTERPRISE OPERATIONS

- Autonomous incident response
- First-contact support resolution
- Candidate screening and scheduling
- Vendor renewal negotiation

INDUSTRY-SPECIFIC

- Real-time prior authorization
- Supply-chain disruption response
- Personalized outage communications
- Multi-jurisdiction permit filing

PUBLIC & CIVIC

- Benefits application guidance
- One-on-one tutoring at scale
- Emergency response coordination
- Public-records request fulfillment

CREATIVE & MEDIA

- Script-to-screen video production
- Game NPCs with memory
- Campaign management, brief to launch
- Source-grounded fact-checking

PHYSICAL WORLD

- Plain-language robot tasking
- Live fleet rerouting
- Photo-based equipment diagnosis
- Building maintenance dispatch

SECURITY & RISK

- Tier-1 SOC triage
- Cross-system fraud investigation
- Continuous red-teaming
- Audit-ready evidence collection

aws TRUSTED SHOPS

Blocking agents is not a solution,
because you would be
blocking legitimate business.

The question should be:
How do you tell good agents from bad ones?

Trust is much more than identity.

Trust signals

Attributes

- Verified operator identity
- Business registration (Handelsregister, LEI)
- Operator age
- KYC verification level
- Verified domain control
- Domain age
- Verified contact points
- Tax / VAT ID verified
- Operator jurisdiction

Attestations

- ISO 27001 (privacy, information security)
- SOC 2
- PCI-DSS
- Sector-specific (FedRAMP, HIPAA, DORA)
- Regulatory licences
- Trustmark seals (e.g., Trusted Shops)
- Hardware attestation (TEE)

Reputation

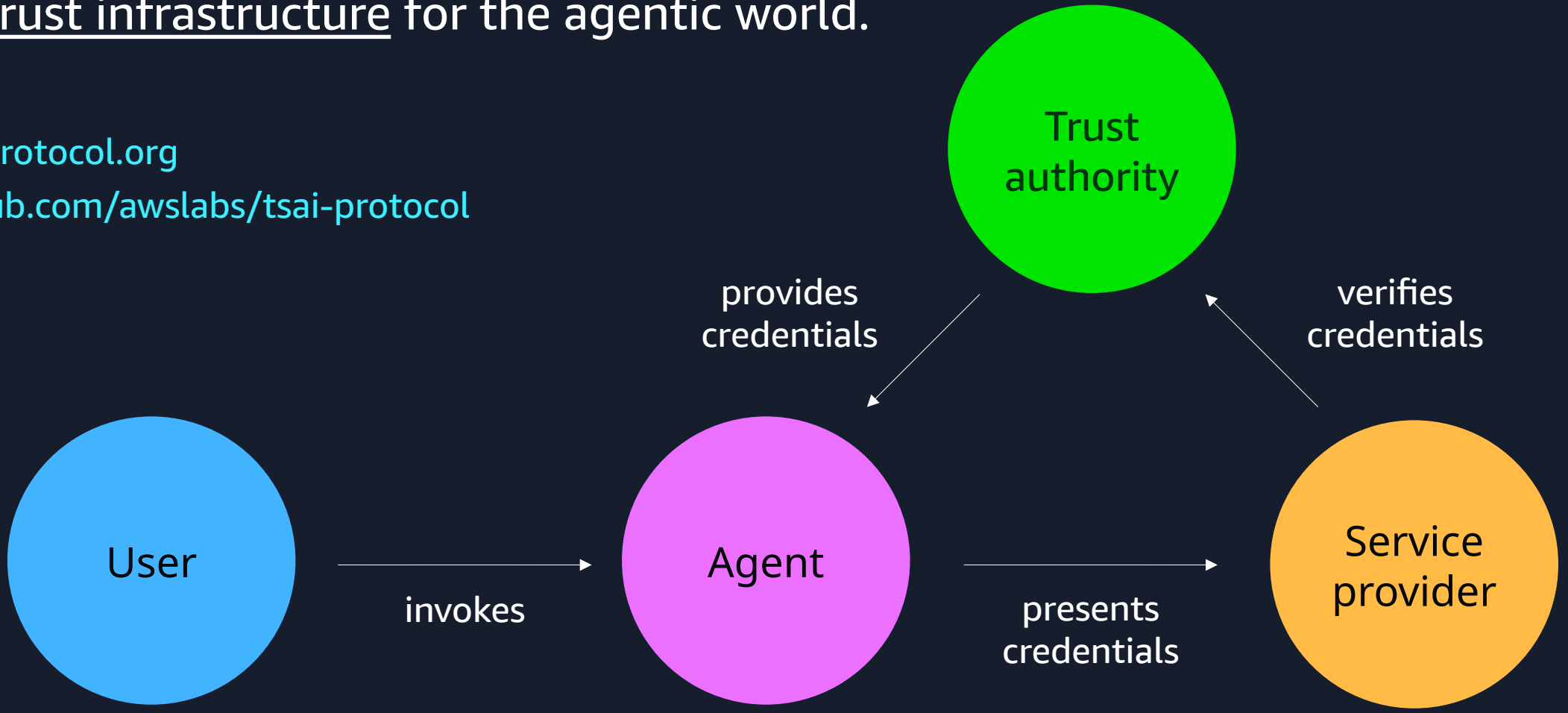
- Task completion rate
- API discipline (429, HATEOAS)
- Directive adherence (agents.txt, robots.txt)
- Access focus (no probing)
- Settlement behaviour
- User satisfaction ratings
- Interaction volume/breadth
- Track-record longevity

Assurances

- Cyber liability insurance
- Professional liability (E&O)
- Bank guarantee or bond
- Posted collateral
- Escrow arrangement
- Buyer protection / refund scheme
- Chargeback protection

TSAI (Trust Signals for Agentic Interactions)
is an industry initiative by AWS and key partners,
building trust infrastructure for the agentic world.

https://tsaiprotocol.org
https://github.com/awslabs/tsai-protocol

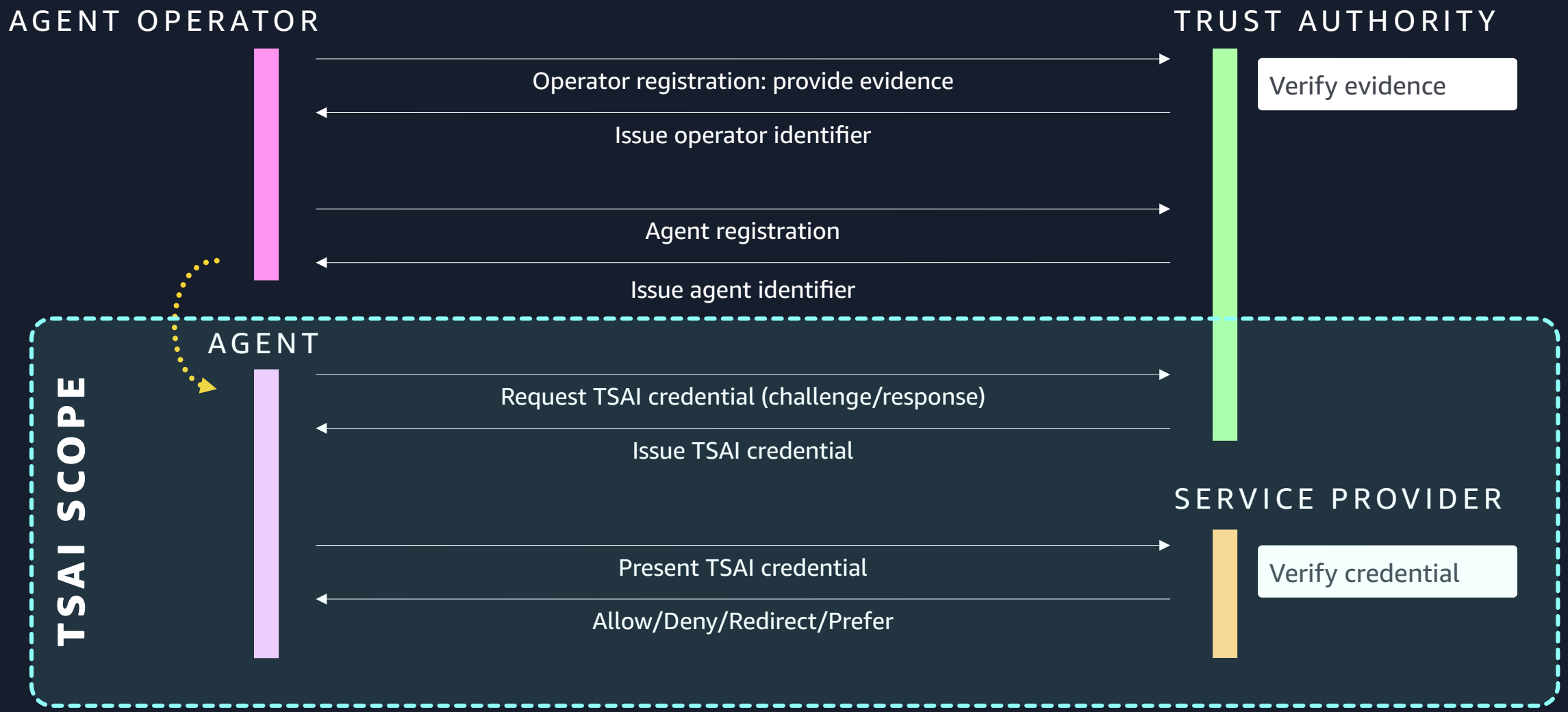


Higher risk needs a higher degree of trust

Trust signal verification (examples)

Category	Signal	Verification
Attribute	Domain	`.well-known` endpoint, domain age
Attribute	Creditcard	Microtransaction
Attribute	Company register	Review entry
Attestation	ISO 27001	Confirm with issuer
Reputation	Transaction count	Feedback mechanism
Reputation	Success score	Feedback mechanism
Assurance	Insurance policy	Confirm with provider

Registration and interaction flows



TSAI: WebBotAuth

Web Bot Auth (WBA)

- Signature of HTTP request
- Based on RFC 9421 (Message Signatures)
- Broad agentic industry support

← INTEGRITY/IDENTITY

SD-JWT

- Selective disclosure of web tokens
- Standardised as RFC 9901
- Verifiable credentials as profile (proposal)

← VERIFIABLE CREDENTIALS

Bringing HTTP standards together

```
POST /checkout HTTP/1.1

Host: shop.example
```

```
Signature: sig=:d2k8v1...raw-64-byte-ed25519-sig...:
```
RFC 9421

```
Content-Digest: sha-256=:X48E9qOo...:
```
RFC 9530

```
Signature-Input: sig=("@method" "@target-uri" "content-digest" "signature-agent")
    ;created=1781863200;expires=1781863260
    ;keyid="Qvnhsitr_LtPwqO7WdAr754JPOYj2mwakhmt8CmZcQ8"
    ;tag="web-bot-auth"
```
RFC 9421

```
Signature-Agent: "https://acme-corp.com"
```
WBA

`TSAI-Credential:` `<issuer-JWT>~<KB-JWT>` *RFC 9901*

SD-JWT credentials

```
{
  "iss": "did:web:trusted-shops.com:tsai:ta",
  "vct": "https://tsaiprotocol.org/spec/tsai",
  "iat": 1781863200,
  "exp": 1781866800,
  "sub": "did:web:example.com:agents:shopper-v3",
  "cnf": {
    "jwk": {
      "kty": "OKP",
      "crv": "Ed25519",
      "x": "Y0bR7h8HbkcM4Ny8J…"
    }
  },

  "signals": […]

}
```

```
"signals": [
  { "cat": "atb", "typ": "dct", "val": "agent.example" },

  { "cat": "atb", "typ": "dag", "val": "P850D" },

  { "cat": "atn", "typ": "iso27001",
    "prv": "cert-corp.example", "exp": 1981863200 },

  { "cat": "rep", "typ": "ecommerce",
    "prv": "rating-agency.example",
    "scr": 0.94, "cnt": 3518, "wdw": "P90D" },

  { "cat": "asr", "typ": "insurance",
    "prv": "cyber-insurance.example",
    "cvr": { "val": 100000, "cur": "EUR" } }
]
```

aws TRUSTED SHOPS

SD-JWT selective disclosures

```
{
  // other fields omitted
  "signals": [
    { "...": "ty59z06I2FA8wqCn_aE6hrvG1QI6VEqUxi2GevjyWds" },
    { "...": "80DjU3lN5ZD6jbIXKhauLSsUQoiVo-rtoOyWo7MKKdg" },
    { "...": "cpOGngkxPgwAXC3m7O9yMnWpg4PERceT1ogU910WXMA" },
    { "...": "R14xFe3IAF6bL9ghFY50YlYiVbbd5AMNsL6iixCHlos" },
    { "...": "KpZwz_z7__1hEEc3c0NF0UaTXfAd_eECi3avqUm_tVQ" }
  ],
  "_sd_alg": "sha-256"
}
```

```
["wZzVnmNt…", {"cat":"atb","typ":"dct","val":"agent.example"}]
["mxDWv3-4…", {"cat":"atb","typ":"dag","val":"P850D"}]
["kV_gv1K8…", {"cat":"atn","typ":"iso27001","prv":"cert-corp.example","exp":1981863200}]
["qS_vWTDx…", {"cat":"rep","typ":"ecommerce","prv":"rating-agency.example","scr":0.94,"cnt":3518,"wdw":"P90D"}]
["7DkJbDZe…", {"cat":"asr","typ":"insurance","prv":"cyber-insurance.example","cvr":{"val":100000,"cur":"EUR"}}]
```

Credential verification by Service Provider

AT THE EDGE

PHASE 1: AGENT AUTHENTICATION

- Parse Signature-Input; check freshness (`created`, `expires`)
- Fetch key directory from Signature-Agent (`/.well-known/...`)
- Locate signing JWK by keyid (SHA-256 thumbprint)
- Verify `Content-Digest` over the body
- Reconstruct signature base and verify signature

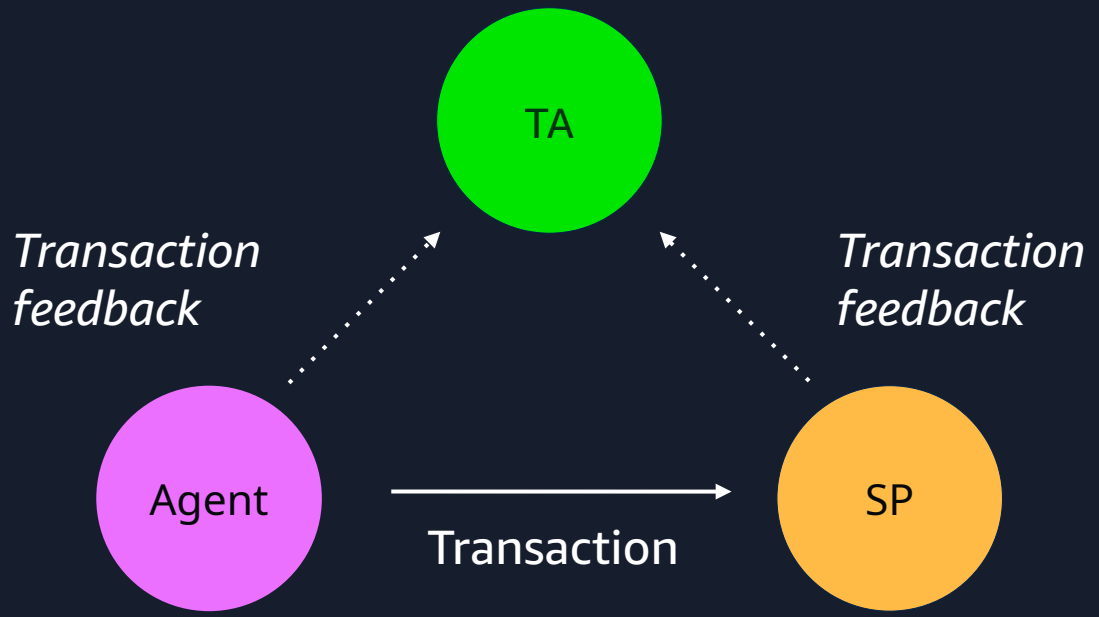
IN THE APPLICATION

PHASE 2: TRUST SIGNALS

- Split TSAI-Credential on ~ (issuer JWT + KB-JWT)
- Fetch TA JWKS (`/.well-known/jwt-vc-issuer`); TA in trust list
- Verify issuer signature; check `exp`, `vct`, `status`
- If SD: Hash disclosures, match against payload's digests; substitute disclosed values.
- Verify KB-JWT signature using `cnf` JWK
- Check `aud`, `nonce`, `iat`, and `sd_hash`
- Evaluate signals against SP policy

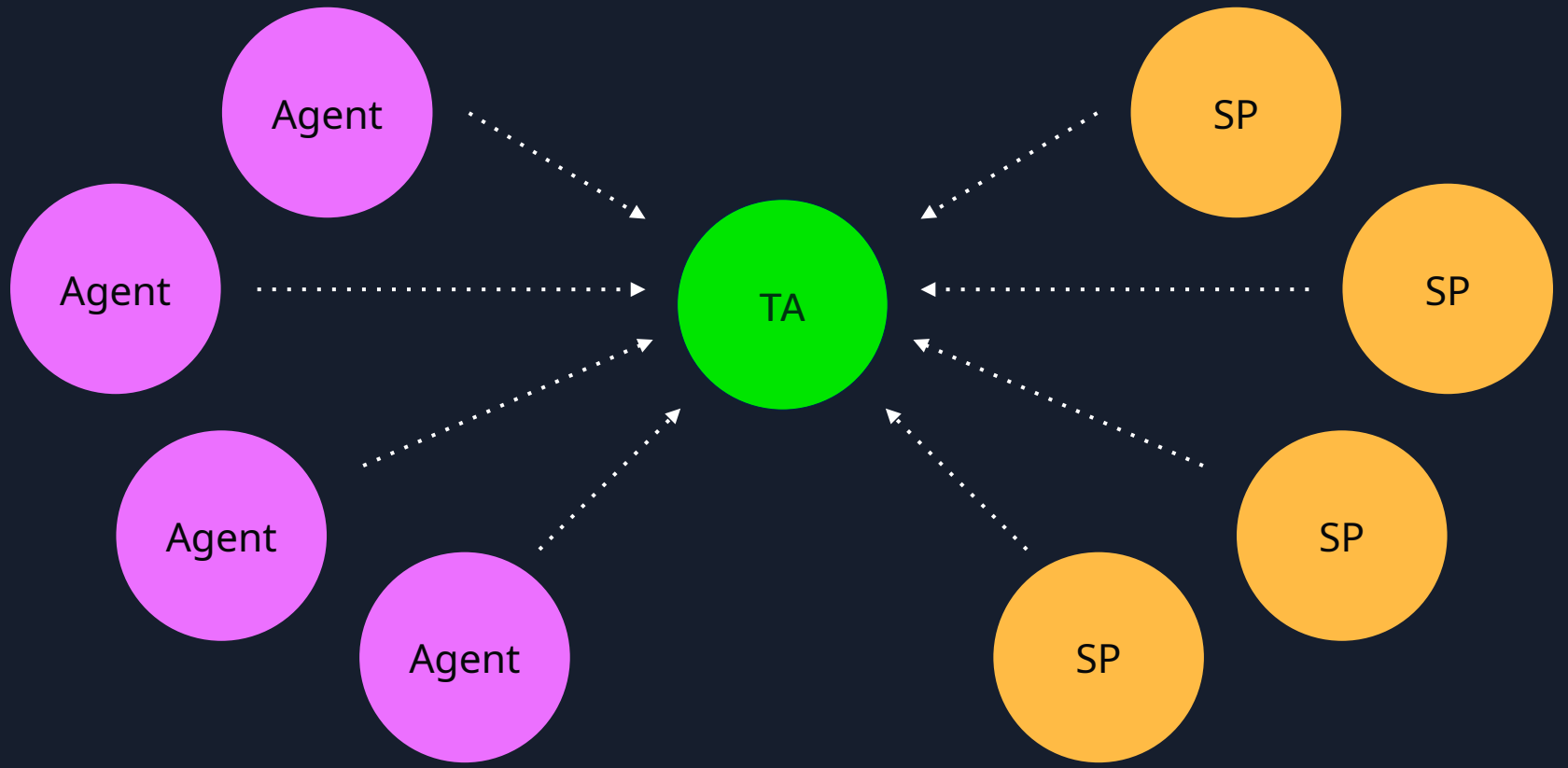
Reputation feedback loop

NOT IN PROTOCOL SCOPE, JUST FOR ILLUSTRATION



Reputation feedback loop

NOT IN PROTOCOL SCOPE, JUST FOR ILLUSTRATION

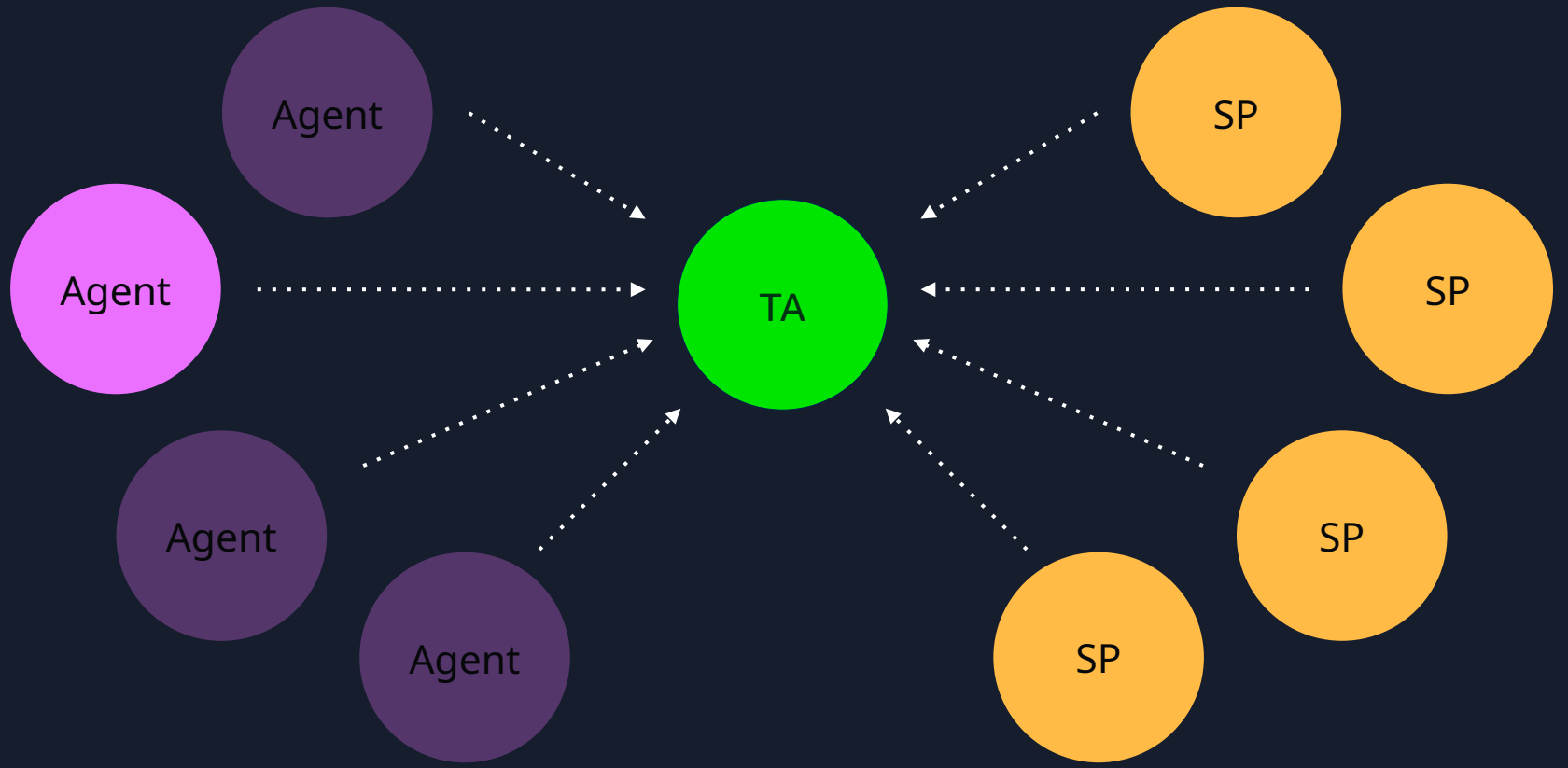


Reputation feedback loop

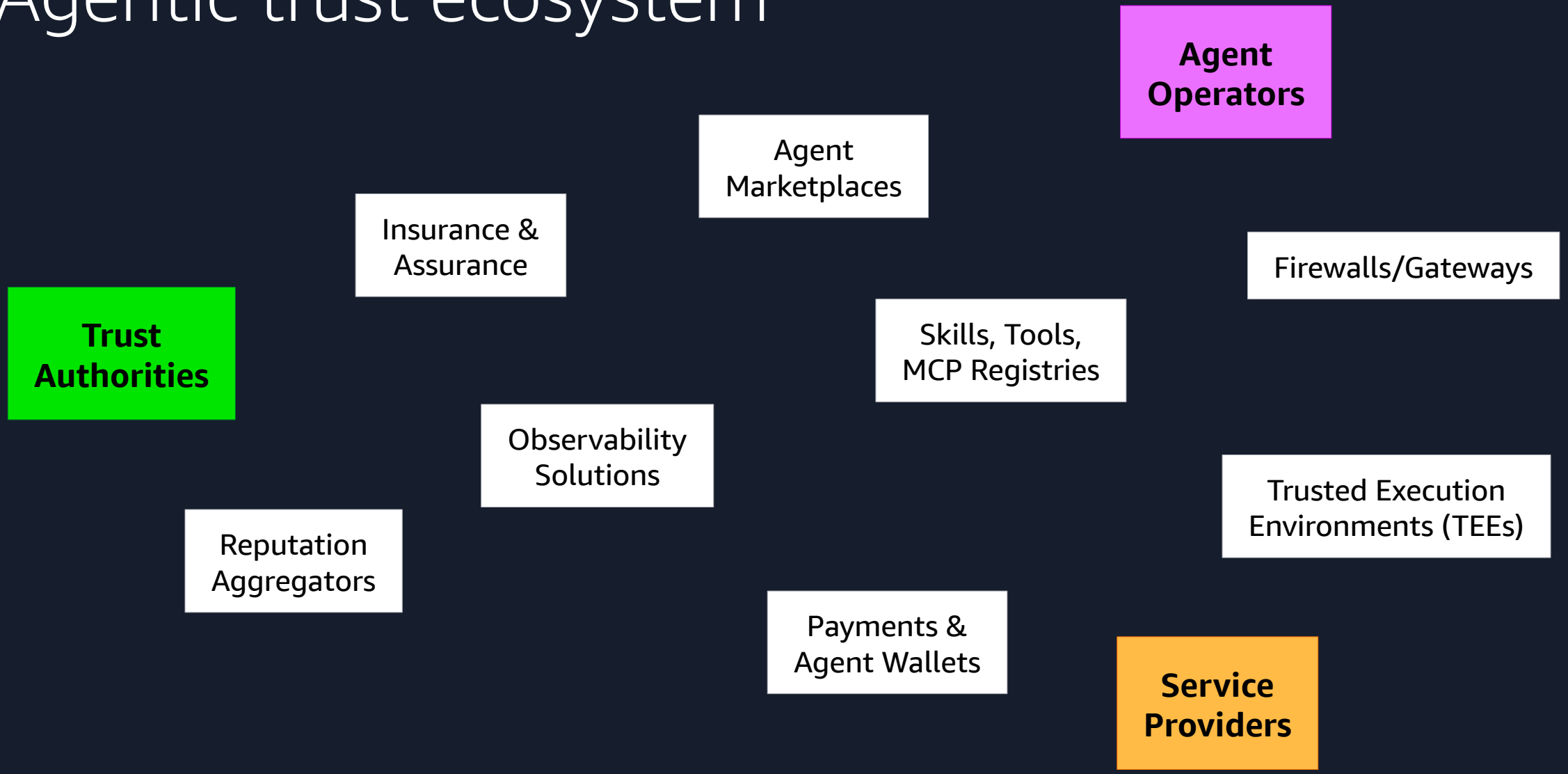
NOT IN PROTOCOL SCOPE, JUST FOR ILLUSTRATION

SP_1	SP_2	SP_3	SP_4	SP_x
0.7	1.0	0.9	0.9	…

```
{
  "scr" : 0.875,
  "cnt" : 4
}
```



Agentic trust ecosystem



Thank you!

Sabrina Engling
sabrina.engling@trustedshops.de
/in/sabrina-engling

Alexander Günsche
lxg@amazon.com
/in/alexander-guensche