MAX-Trust: Toward a Unified Trust Framework for Next-Generation Agent-Driven Communication Networks

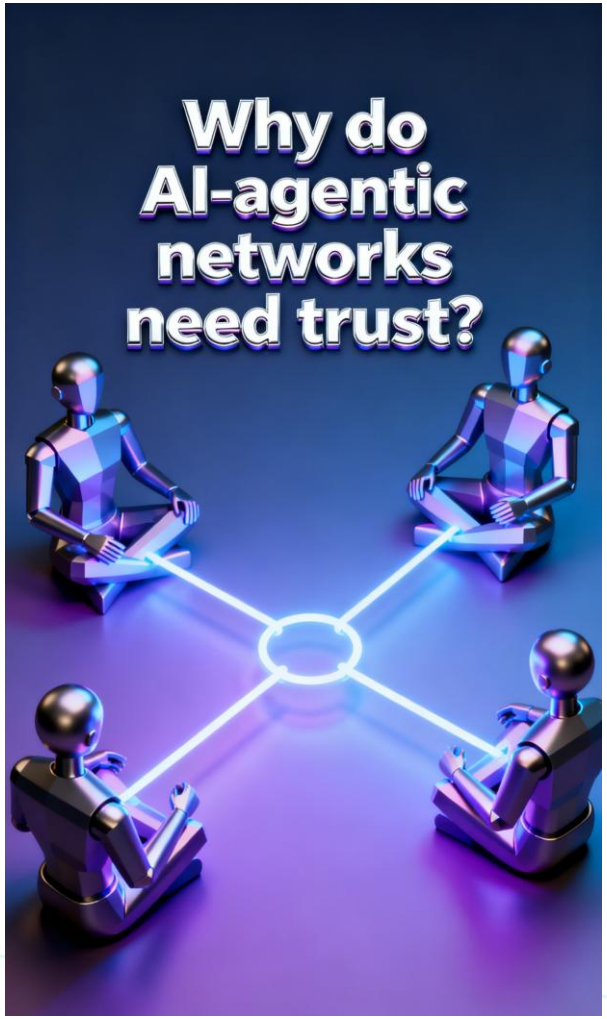
Speaker : Kang Xin, Huawei Singapore Research Center

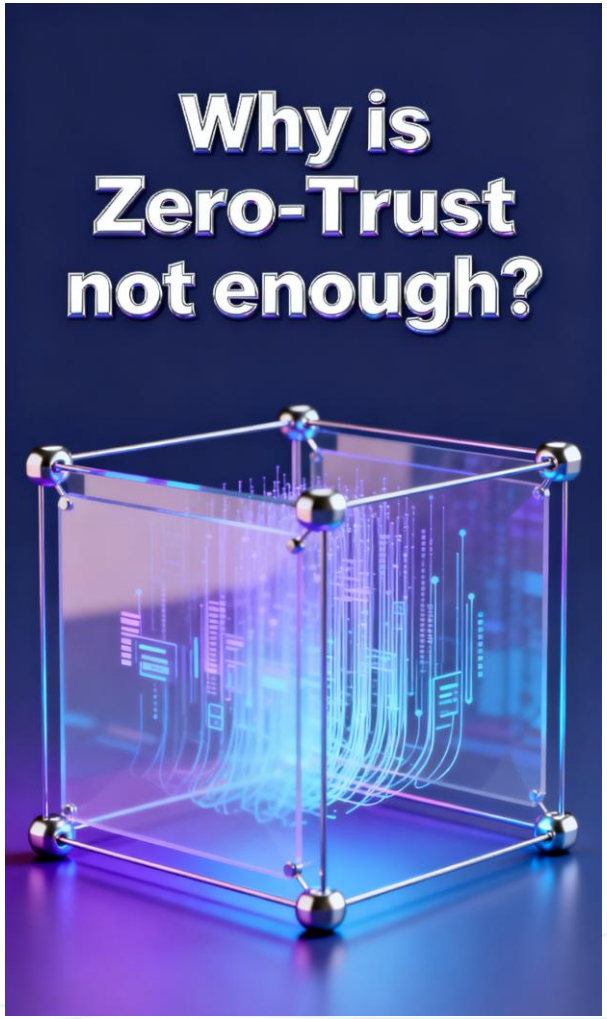
Date : 2026.03.30

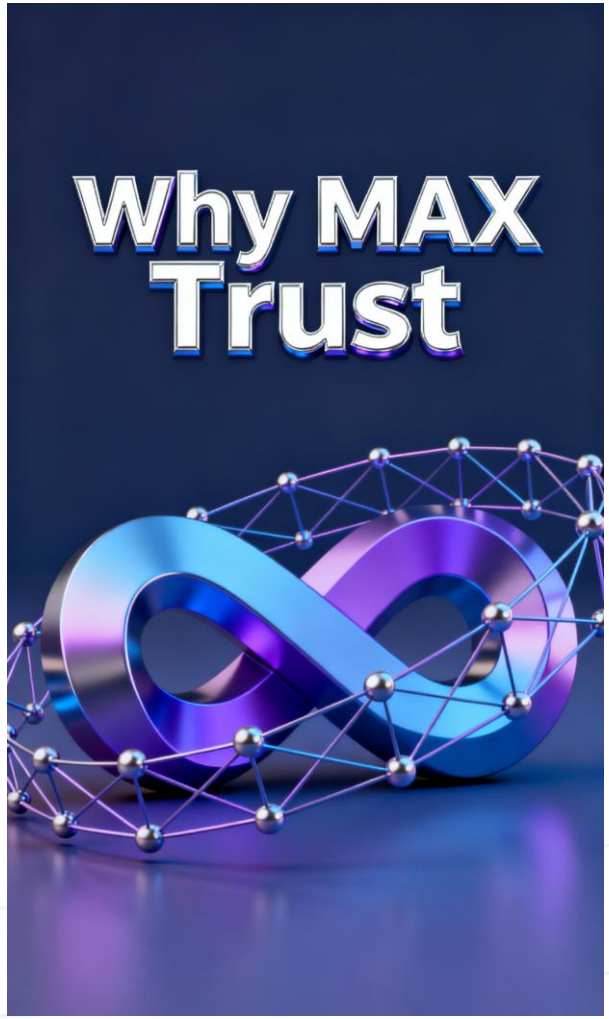
Security Level:

HUAWEI

Content


Why do AI-agentic networks need trust?


Why is Zero-Trust not enough?


Why MAX Trust

Core Concept of Trust

Trust propensity
Trustor's generalized expectation about trustees

Trustworthiness
Reliability of trustee to trustor

Trustor — **Trustee**

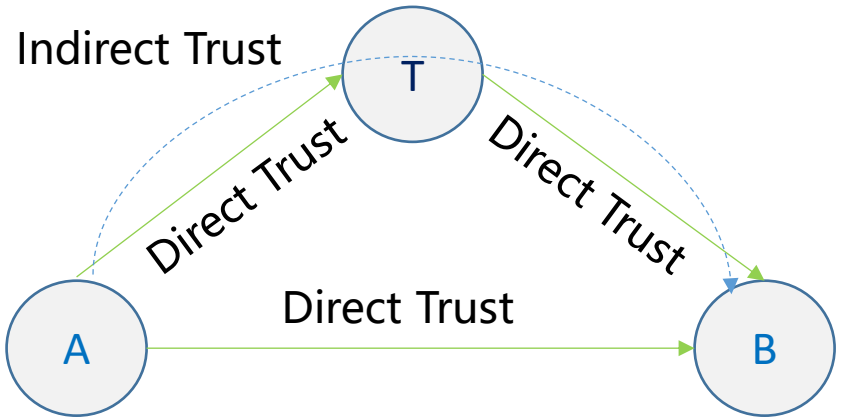
Trust

Direct Trust — **Indirect Trust**

Knowledge
Own understanding about trustee

Experience
Personal expertise about situation and context gained from previous experience with trustee

Reputation
Public evidence about trustee based on experiences of all trustors with trustee



Properties and Functions of Trust

Easier to lose than to gain

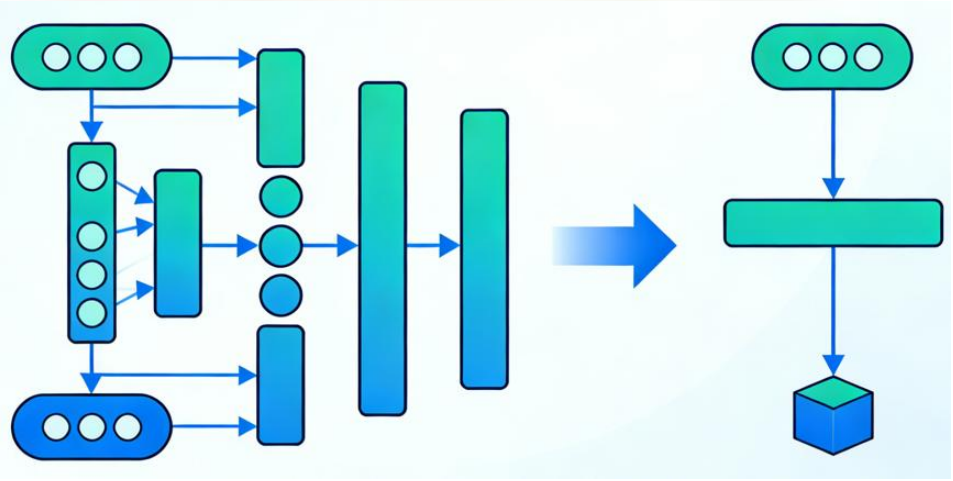
Context dependent

Asymmetric

Subjective

Dynamic

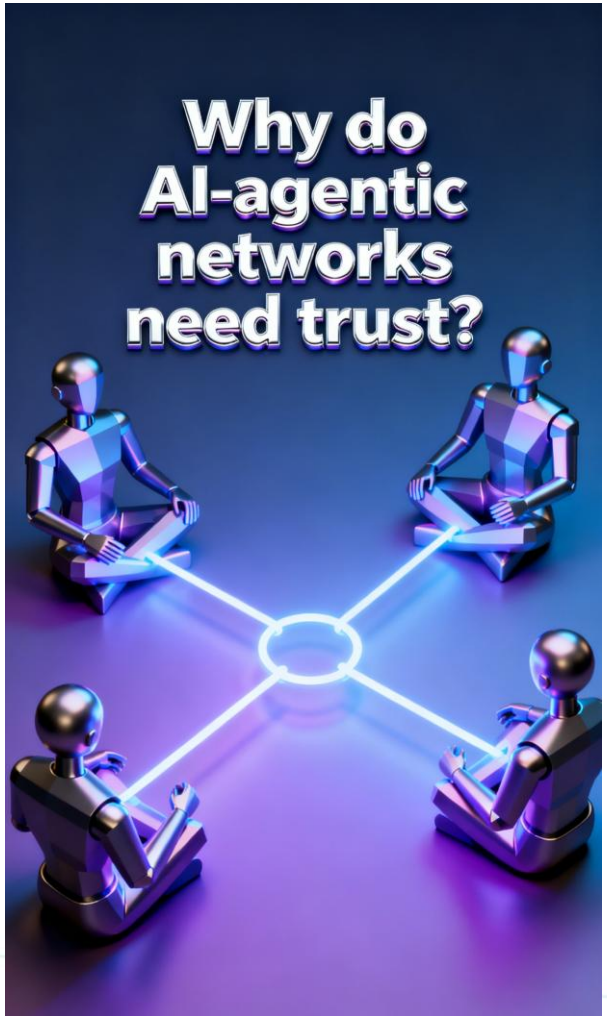
Transitive



Simplify System Design

Facilitate Cooperation

Content


Why do AI-agentic networks need trust?


Why is Zero-Trust not enough?

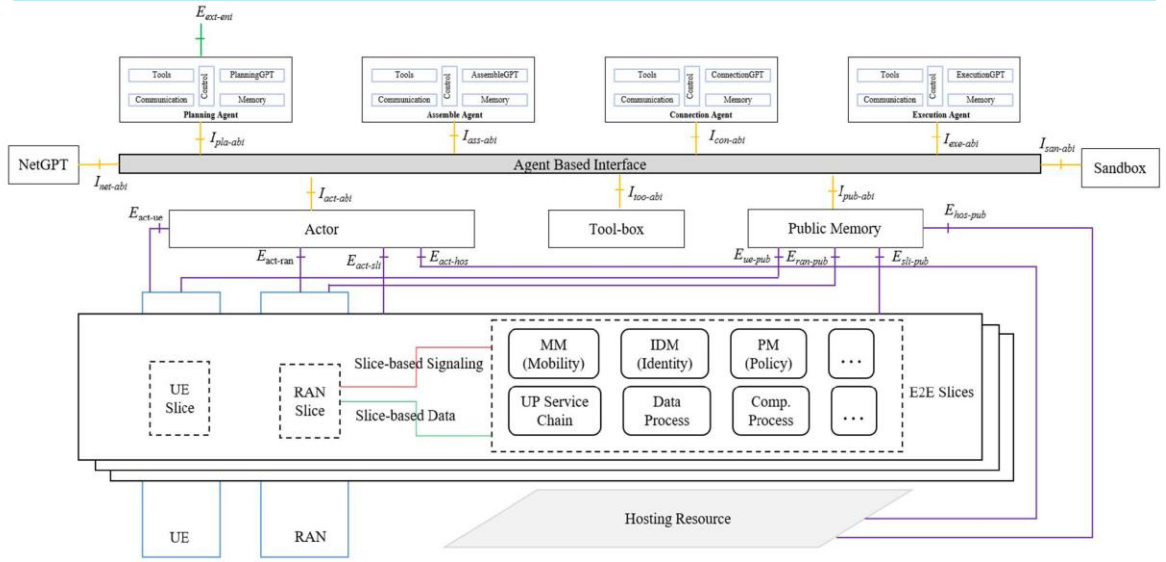
Why MAX Trust

Architecture Changes Pose New Challenges on Security

6G System Design Considerations

- **Focus and Simplicity**
  - Lean and streamlined standards for 6G, e.g., by dimensioning an appropriate set of functionalities, minimizing the adoption of multiple options for the same functionality, avoiding excessive configurations, etc.
- **Cloud-Native Architecture**
  - Designing networks to be cloud-native to enable flexibility, agility, and innovation.
- **AI-Native Design**
  - Integrating AI and ML frameworks natively into the network for intelligent automation, optimization, and improved efficiency.
- **Scalability and Modular Design**
  - Implementing a scalable and modular design that allows a wide range of features, device types, services, and spectrum bands to be developed and deployed as needed.
- **Software-Driven Deployment**
  - Software-driven deployment with needs-based hardware refresh to allow for continuous innovation and agility.
- **Interoperability**
  - Designing components with interoperable interfaces and a unified management framework to ensure interoperability and avoid fragmentation.
- **Enhanced Security**
  - Ensuring the 6G system is secure by design to provide enhanced security and privacy.
- **IoT Support**
  - Designing 6G to support diverse IoT device types and use cases from day one, with a focus on long-term commitments and multi-generational solutions.
- **Service-Aware**
  - Enabling a service-aware intelligent network powered by AI-native, programmable, and service-aware 6G RAN.
- **Ubiquitous Connectivity**
  - Providing ubiquitous coverage through seamless integration of terrestrial and non-terrestrial networks.

Source: Chair Summary of 3GPP Workshop on 6G (2025.03)



Source: Huawei《6G: The Next Horizon》white paper

Source: ETSI- AI Core Reference Architecture (2025.02)

*GR ENI 051-Study on AI Agents based Next-generation Network Slicing

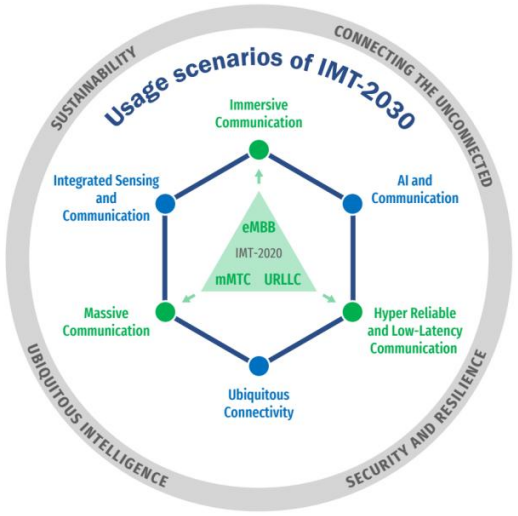
The **Agentic-AI 6G architecture** design poses new challenges on security:

- Challenge 1: Probabilistic decision-making of AI may bring uncertainty
- Challenge 2: The autonomy of Agent may lead to issues such as intention/value misalignment

✓ **Traditional security measures may not be adequate** (e.g. static security domains, focusing on external attacks)

✓ **Trust is considered to be a feasible solution** (e.g. value alignment, liability linkage)

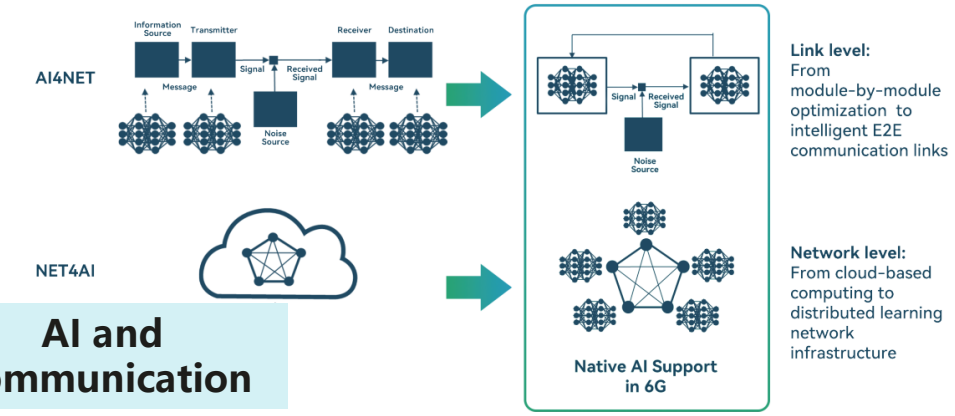
New Usage Scenarios Bring out Strong Trust Needs



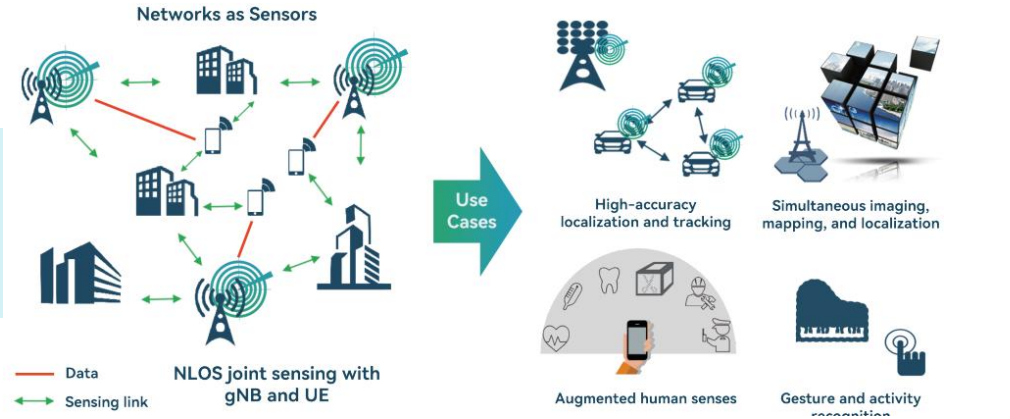
Source: ITU-R M.2160-0 (11/2023)

*Framework and overall objectives of the future development of IMT for 2030 and beyond

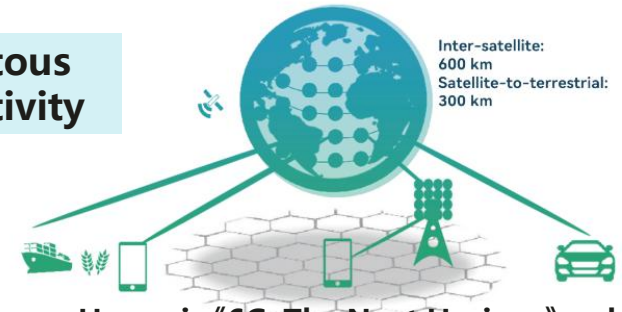
1 AI and Communication



2 ISAC



3 Ubiquitous Connectivity



Source: Huawei《6G: The Next Horizon》white paper

Trust Requirements of 6G

1 AI and Communication

- Mutual trust among Agents
- Mutual trust between Human and Agents

2 Integrated Sensing and Communication

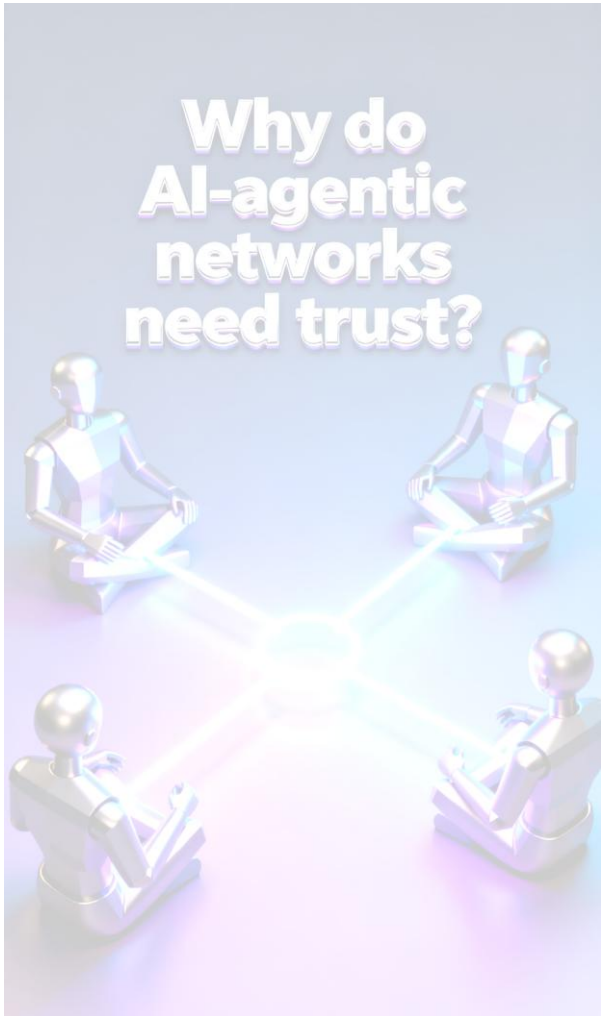
- Data Trustworthiness
- Data Privacy Protection
- Trustworthy data sharing among multi-parties

3 Ubiquitous Connectivity

- Mutual trust among Multi-domains
- Mutual trust among heterogeneous networks

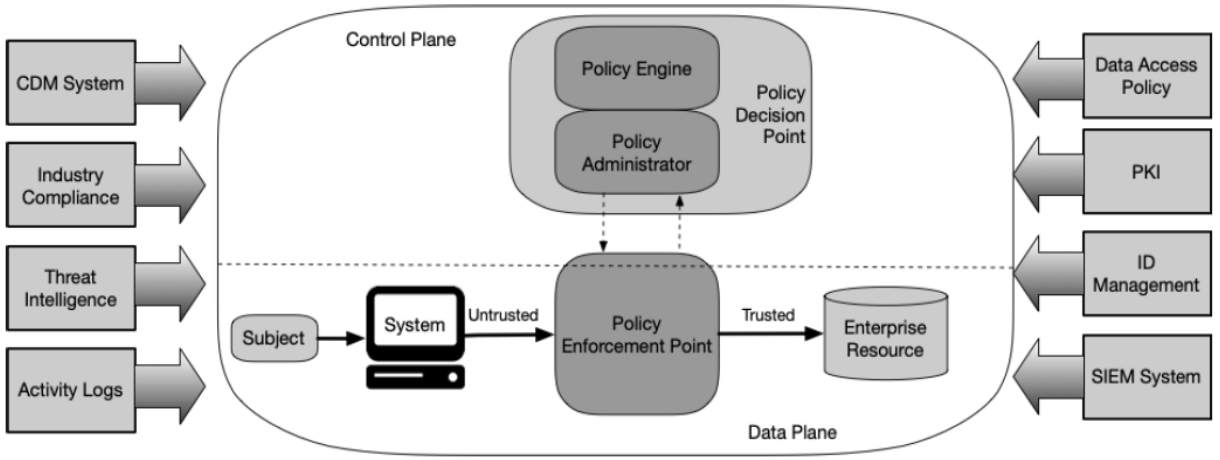
6G's new services are deeply integrated with AI; shifting from "point by point defense" to "systematic trust" is success key.

Content



Revisit Zero Trust

Zero Trust Architecture



Source: NIST Special Publication 800-207 《Zero Trust Architecture》

- Continuous diagnostics and mitigation (CDM) system
- Industry compliance system
- Threat intelligence feed(s)
- Network and system activity logs
- Data access policies
- Enterprise public key infrastructure (PKI)
- ID management system
- Security information and event management system

Zero Trust Tenets

Seven basic tenets identified by NIST

1. All data sources and computing services are considered resources.
2. All communication is secured regardless of network location.
3. Access to individual enterprise resources is granted on a per-session basis.
4. Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes.
5. The enterprise monitors and measures the integrity and security posture of all owned and associated assets.
6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed.
7. The enterprise collects as much information as possible about the current state of assets, network infrastructure, and communications and uses it to improve its security posture.[3]

Zero Trust Key Approaches

Least Privilege
Grant only minimal access needed for tasks

Continuous Monitoring
to timely identify abnormal activities, ensure immediate response to threats

Identity-Centric
uses the identity of actors as the key component of policy creation

Can we apply the zero trust technologies directly to the future AI-Agentic network design?

Challenges When Applying Zero Trust to Future AI-agentic Networks

Performance & User Experience

Zero Trust relies on continuous verification, but in highly dynamic AI environments, frequent verification may consume significant computing resources, introduce latency, and impact network performance and user experience.

User Privacy

Zero Trust requires collecting large amounts of user behavior data for risk assessment, yet in 6G scenarios, requirements for privacy protection (such as the EU's GDPR) may restrict the scope of data usage,

AI Uncertainty

Faced with the AI-driven nature of 6G, AI systems' behaviors may go beyond preset rules (e.g., the output of generative AI), and the rule engine of traditional Zero Trust struggles to cover all potential risks.

Autonomous Decision-Making

Under the trend of Agentic-AI, network entities have enhanced autonomous decision-making capabilities, which requires highly autonomous data access capabilities, while least privilege rule may restrict their flexibility.

Multi-Domain & Multi-Network

Zero Trust, initially proposed for enterprise networks, struggles with the fact that the trust logic of a single domain failing to adapt to the complexity and diversity of multi-domain & multi-network case of 6G

M-Trust (Multi-Trust)

- **Multi-party Trust**: Involves multi-party participation in evaluation/verification, and Eliminates dependence on a single point
- **Multi-mode Trust**: Supports multiple trust modes such as authority-based, endorsement, and consensus

A-Trust (Agentic Trust)

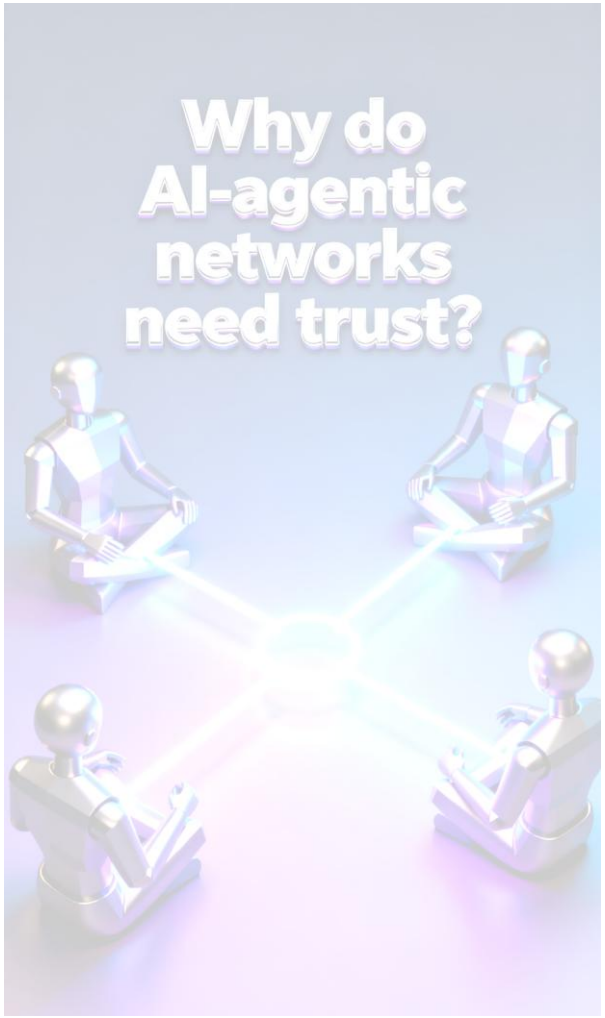
- **Agile Intelligent Triggering:** Flexibly adjust trust assessment requirements/ algorithms based on scenarios and risks
- **Intelligent Policy Configuration:** Agents automate policy configuration to simplify complexity

X-Trust (Xross Trust)

- **Heterogeneous Trust Root:** Expands trust sources; trust may come from hardware, software, or infrastructure
- **Cross-domain Trust:** Achieve seamless trust transfer across multi-domain/multi-network scenarios to eliminate redundant verification

A migration from zero-trust to a high-dimensional trust (MAX-Trust) deep integrated with Agentic-AI is needed for 6G

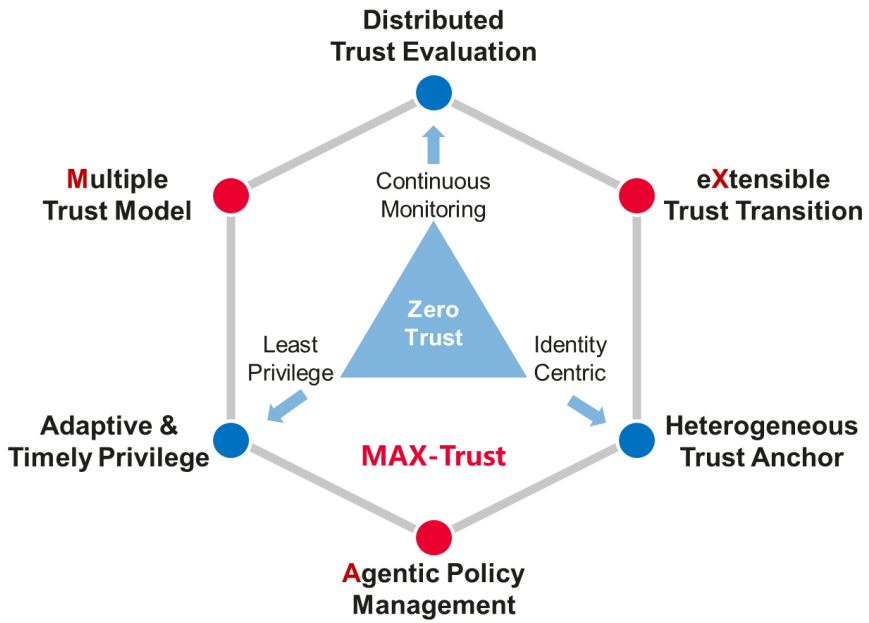
Content



HUAWEI

A Paradigm Shift From Zero-Trust to MAX-Trust

Core Principles of MAX-Trust

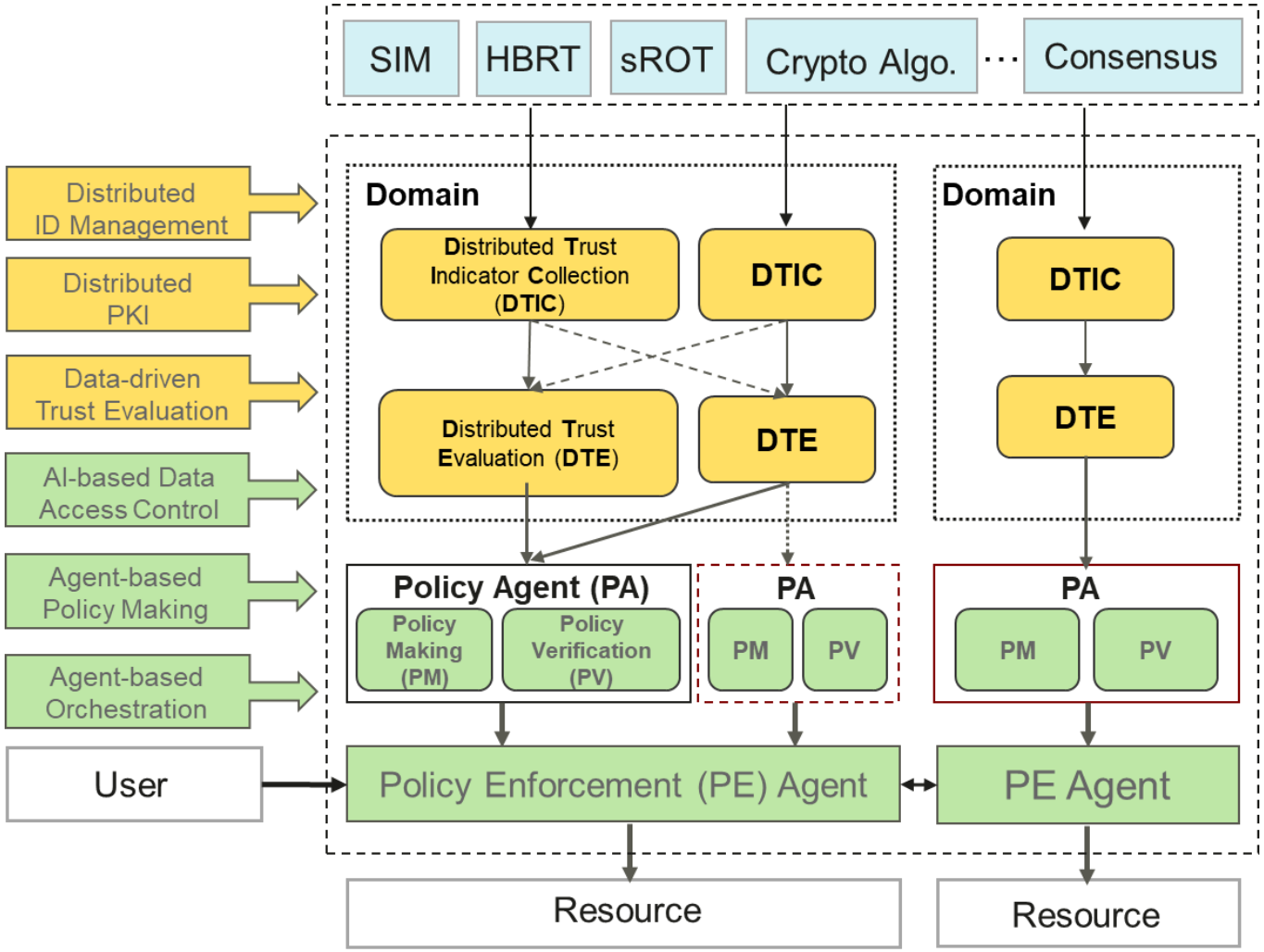


Multi-Party, Co-Governance

Agentic, Intelligent

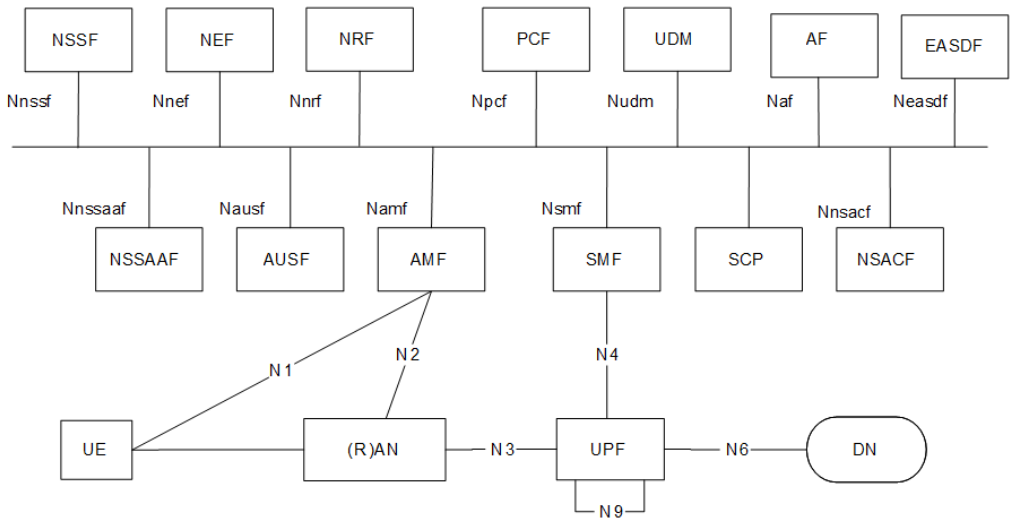
eXtensible, Heterogeneous

High-Level Architecture of MAX-Trust

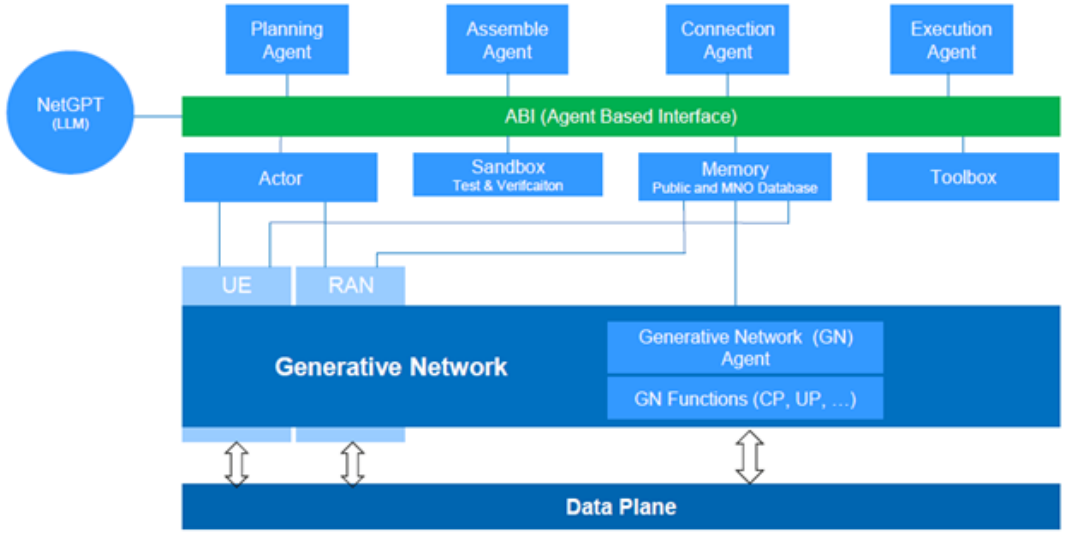


HUAWEI

Integrate MAX-Trust to the Agent-based Future Network



Source: 3GPP TS. 23.501 System Architecture for the 5G system



Source: 3GPP 6G Workshop (2025.03)

Enabling Technologies of MAX-Trust

M-TRUST Principles & Components

- **Trust Relationship**: Federated; Decentralized
- **Trustworthy Architecture**: Distributed; DPKI
- **Trustworthy Protocols**: 6G-AKA; EAP-TLS+

A-TRUST Principles & Components

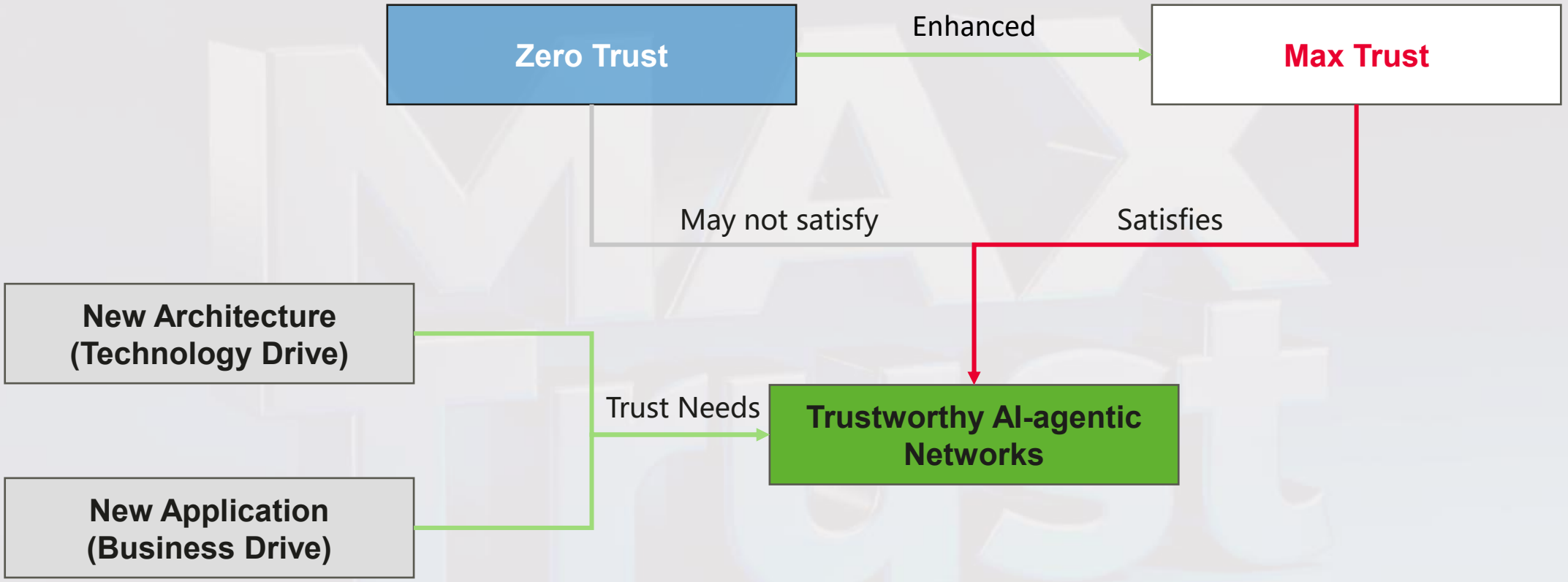
- **Trustworthy AI**: Privacy-preserving; Explainable; Unbiased
- **Trust Evaluation**: Static; Dynamic
- **Trustworthy Underlay**: Autonomous; NFV/NFVI

X-TRUST Principles & Components

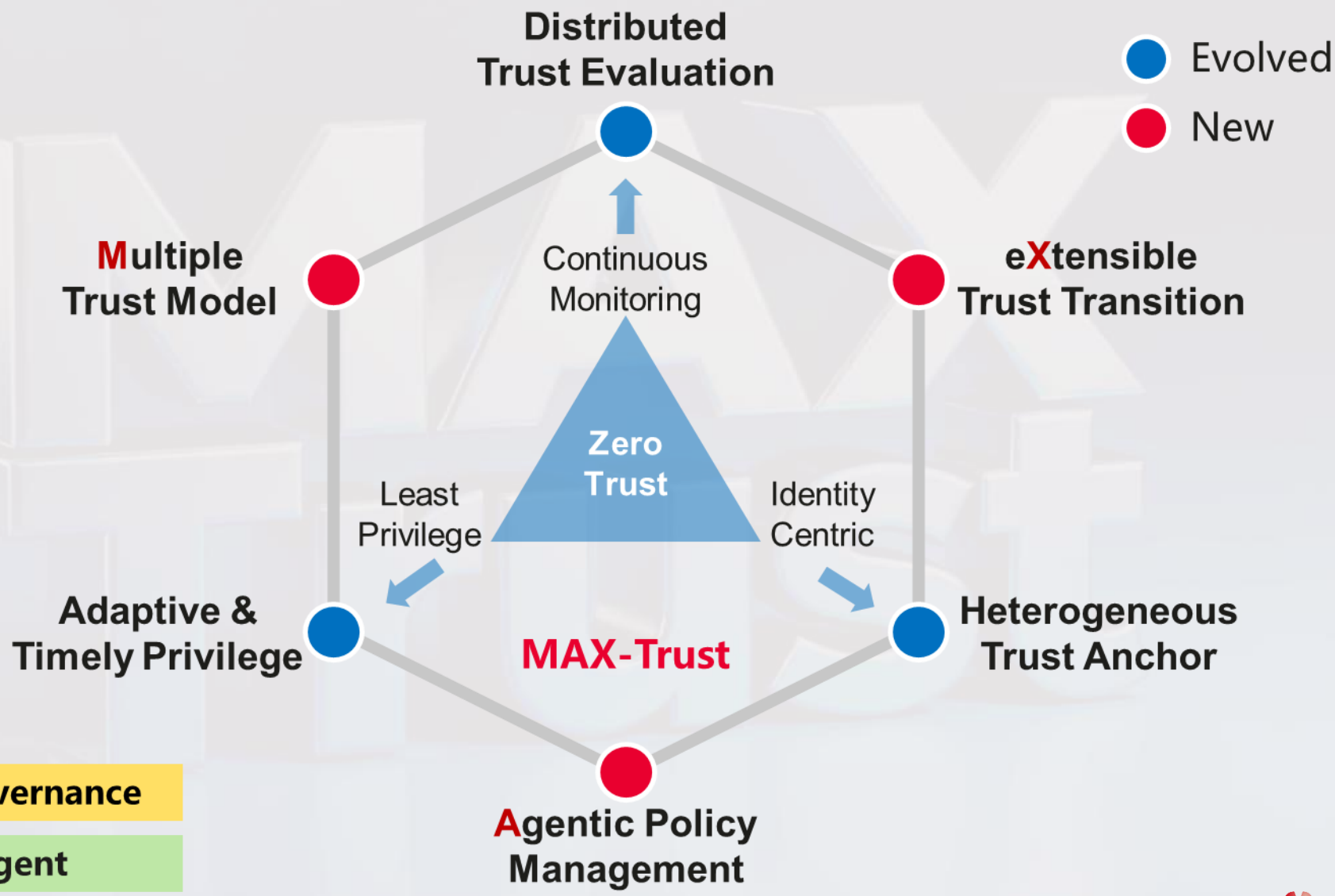
- **Trust Anchor**: HBRT; eSIM/SIM; sRoT
- **Trust Foundation**: Symmetric Crypto; Asymmetric Crypto
- **Trust Platform**: TEE; Blockchain

Directly applying the zero-trust to the future Agentic-AI based network may not be the optimal solution, a high-dimensional trust deeply integrated with Agentic-AI is needed for the future network

Conclusions



MAX-Trust for Agent-driven Networks



Multi-Party, Co-Governance

Agentic, Intelligent

eXtensible, Heterogeneous

HUAWEI

Thank you.

Bring digital to every person, home and organization for a fully connected, intelligent world.