

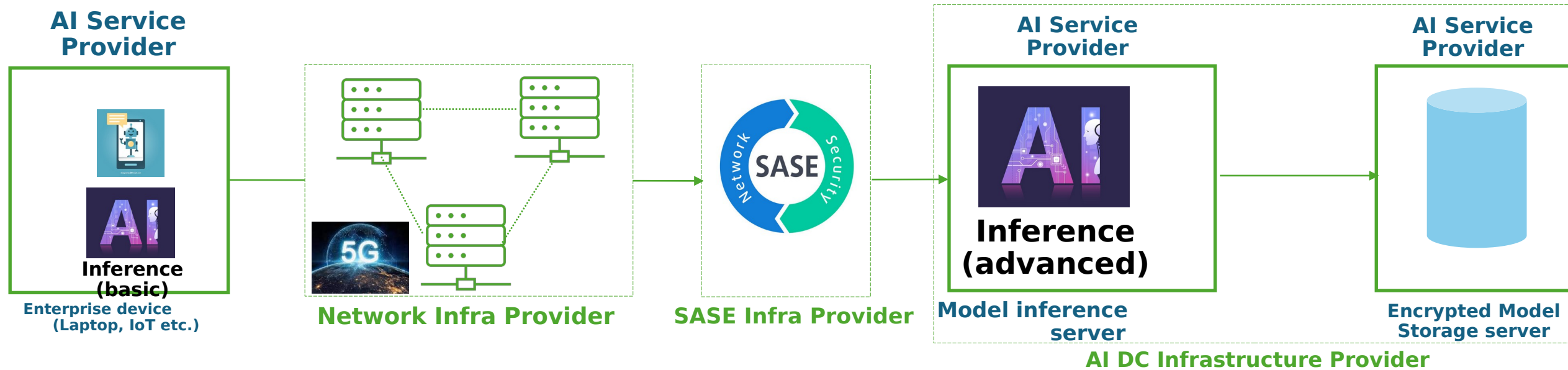
End-to-end multi-vendor, multi-cloud use cases (AI and beyond) which require NASR

IETF presentation

Ramki Krishnan (Intel), Diego Lopez (Telefonica)

AI Inference accountability across multi-vendors/clouds

Problem statement



Problem background

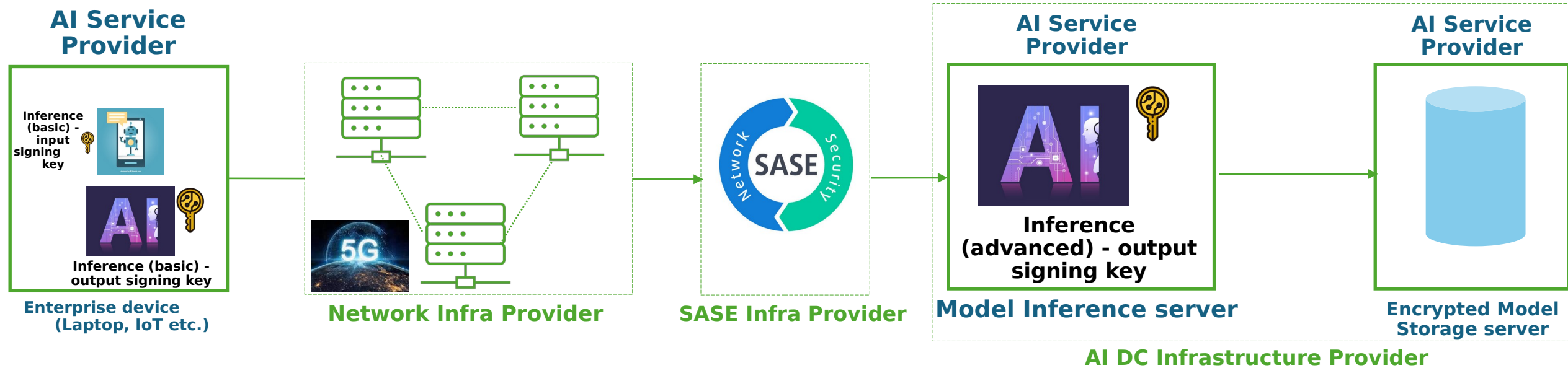
- AI inference output may not be deterministic for the same input (exception is AI expert system), unlike traditional keyword-based lookup.
- SASE, which terminates TLS connections, is typically used to ensure policy compliance and block malicious traffic. SASE may be appending/modifying/filtering Enterprise application payload.
- **Networking infrastructure is a critical piece to ensure availability.**

Problem statement

- Service providers would like to ensure that for every AI inference input, Enterprise customers can
 - Isolate between an AI inference application issue vs SASE infrastructure issue.
 - Verify AI inference input provenance.
 - Verify AI inference output provenance/compliance.
- Service providers would like to ensure that for every AI inference input, 3rd party auditors can
 - Verify AI inference input provenance.
 - Verify AI inference output provenance.
- **Service providers would like to ensure that the routing infrastructure is trustworthy.**

AI inference accountability across multi-vendors/clouds

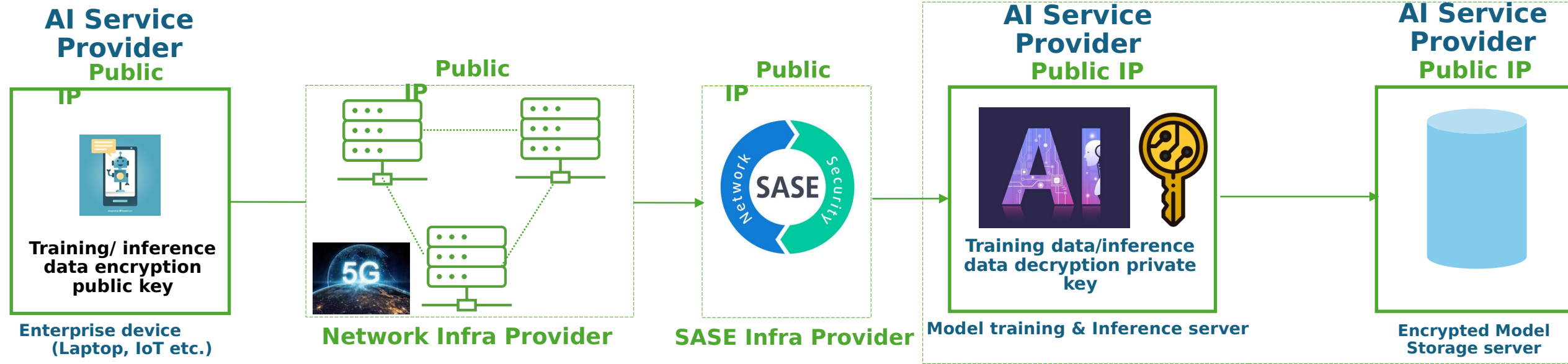
Solution



- After AI Inference processing is complete and before responding to client, store signed AI Inference input and output in a tamper proof audit log
 - Store AI inference input and output signatures in Audit Log Transparency Service
- After SASE processing is complete and before responding to client, store signed SASE processing input and output in a tamper proof audit log if SASE appends/modifies/filters Enterprise application payload.
 - Store SASE inference input and output signatures in Audit Log Transparency Service
- **NASR ensures that the routing system is integrity protected**
 - **Store routing BGP connection source/destination router signatures in Audit Log Transparency Service**
- Audit Log Transparency Service is open to the public for reads like Certificate Transparency Service or Public Blockchains (e.g., Public Ethereum) and can be used to verify AI inference input/output provenance and **Router source/destination provenance**. This uses an Identity/Policy Transparency service which has public shareable Enterprise identities (e.g., workload code hash/signing public key certificate, host TPM public key certificate) and Enterprise Policies (e.g., workload can run only on certain hosts which is achieved by binding workload/host identities).

AI/Other workload proof of data residency across multi-vendors/clouds

Problem statement



- Provide proof to Enterprise customers/3rd party auditors that AI inference/training data is processed only in certain geographical region, e.g., city or country.
- Provide proof to Enterprise customers/3rd party auditors that AI inference/training transit data does not leave a certain geographical region, e.g., city or country – transit data has valuable IP address/Layer 4 port information though the application data is encrypted.
 - As consequence of applying privacy legislation, such as EU GDPR or German BDSG, or healthcare regulation like US HIPPA. As consequence of applying corporate policies regarding data confidentiality

AI/Other workload proof of data residency across multi-vendors/clouds

Solution

- **NASR ensures that the routing system is integrity protected:**
 - **Router management plane can verify authenticity of router workload/network device identity/policy using Identity/Policy transparency service.**
- SAVNET ensures that the source IP has not be tampered with (or spoofed):
 - Each system (end user device, router, SASE, Model training & inference server, Encrypted Model Storage server) is allocated a unique IPv6 address which is location based.
- Confidential computing:
 - Confidential computing hardware (TEE) provides runtime proof that the workload identity (code hash, public key certificate) have not been tampered with.
 - This provides superior security/trust to all workloads – router etc.