Establishing Trust in the Cloud:
Trusted Multi-Tenant Infrastructure

September 2014

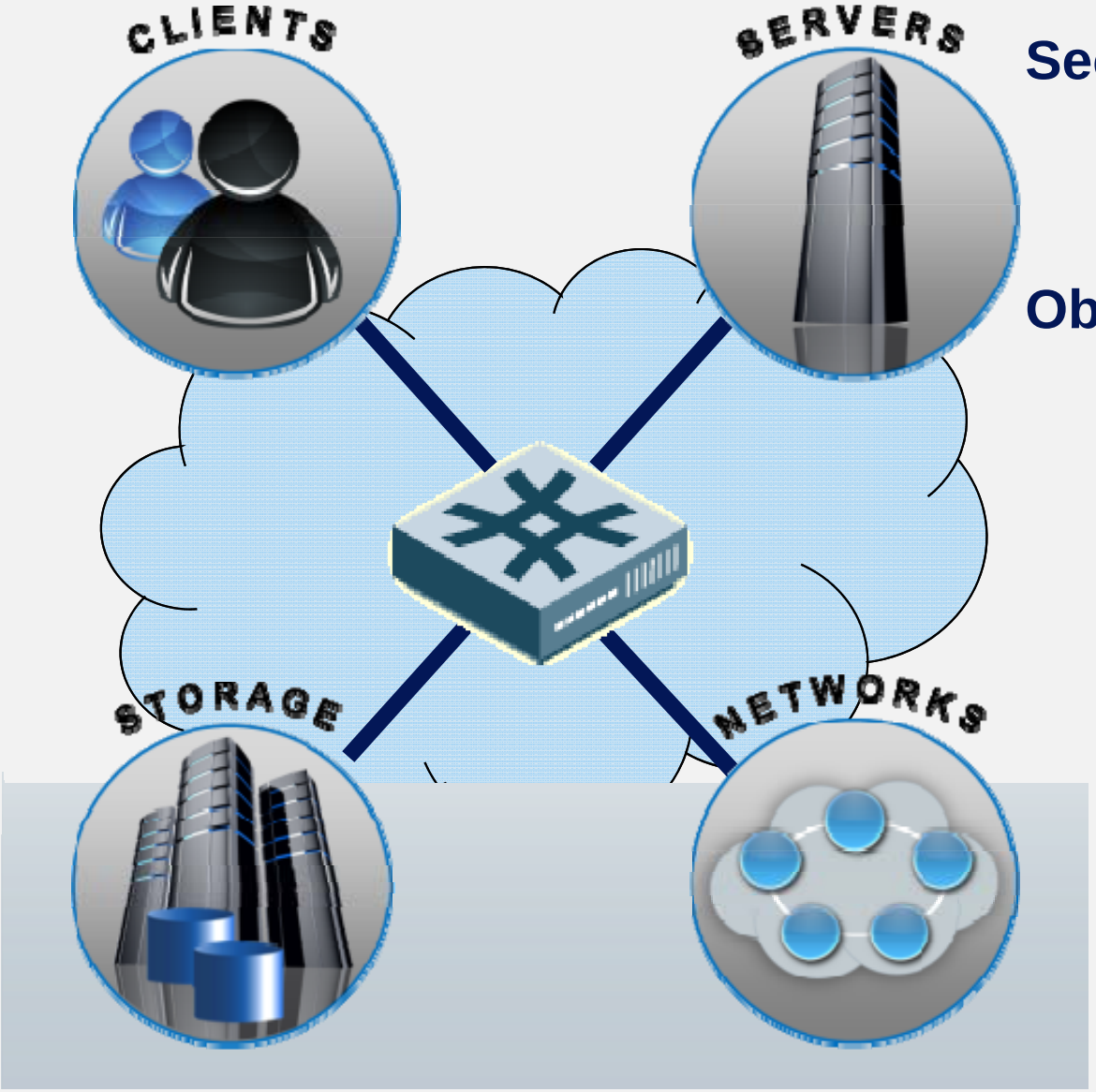
Market Observations

- Multi-Tenant security is an end-to-end configuration requirement, while most of the products and standards address specific devices or functionality within the overall end-to-end scope
- Many standards and products contribute to the ability to solve parts of the problem
- No comprehensive framework exists to describe the business/mission needs and validate compliance of the entire solution set against open standards
- There is a need for solutions that address trust and security across solutions derived from combining dedicated and shared infrastructures

Market Changes

- Cost reduction and IT agility
- Consolidation of IT resources and staffing
- Movement from CAPEX to OPEX funding of IT
- To support shared infrastructure for critical systems:
  - Financial (PCI), Healthcare (HIPAA), Energy (NERC/CIP)
  - Global Government and Industrial Base
  - Defense including joint service or coalition operations
  - Shared services within public, private, community and hybrid cloud solutions
  - Applications supporting the mobile ecosystem

Trusted Platform Framework



Security Built In & Coordinated

- Trusted Multi-Tenant Infrastructure (TMI)

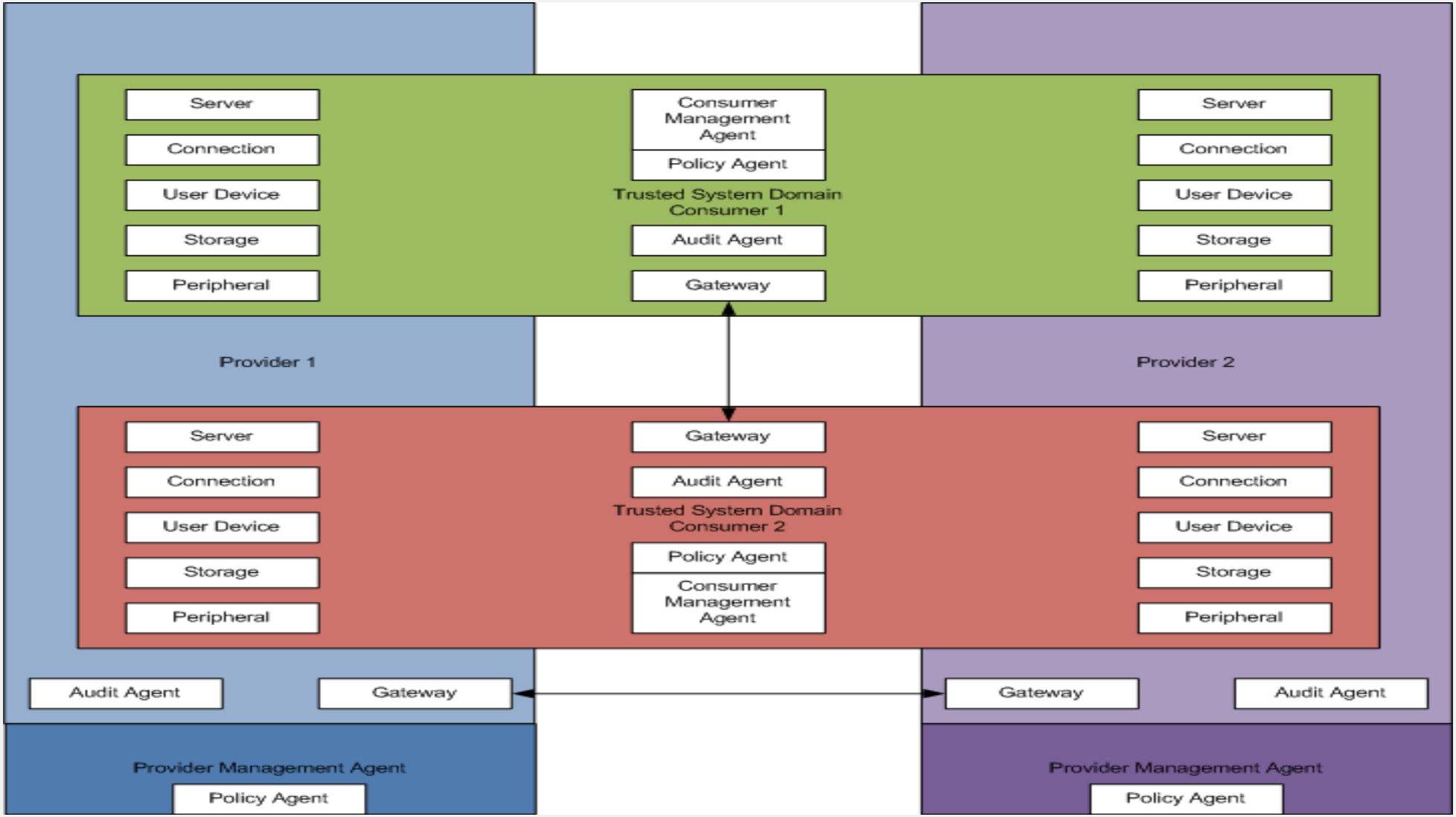
Objectives

- Standards framework for implementing:
  - Shared Infrastructures
  - Multi-Provider Infrastructures
- Reference Models and Implementation Guidance
- Identify and address gaps in existing standards

TMI Reference Model: Core Concepts

- Establish a Trusted Context in which information can be exchanged between parties
  - Establish a level of trust (including the degree and types of information to be accepted) between parties
- Exchange Information between parties within the trusted context
  - Exchange information between parties within the bounds of the trust relationship
- Enforce Policy using the integrity measurements, assertions and attestations exchanged between parties
  - Identify executable policy statements and stores, information sources and sinks, decision authorities, execution points, obligations on parties and policy hierarchies

TMI Reference Model

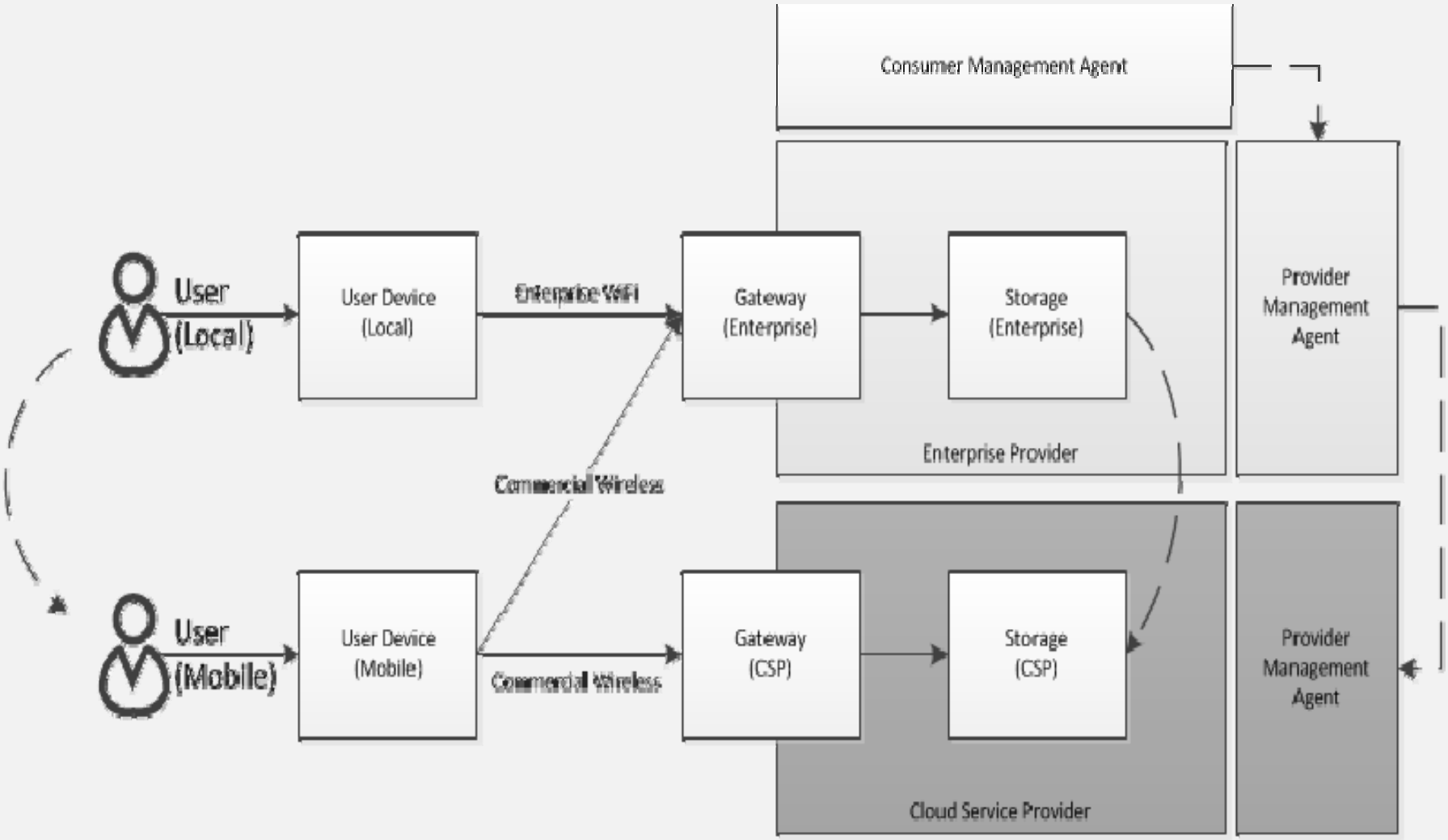


TMI Trust Maturity Model

	Potential Impact								
	Low			Medium			High		
	Likelihood			Likelihood			Likelihood		
	Low	Med	High	Low	Med	High	Low	Med	High
Inconvience-1	T1	T2	T2	T2	T3	T3	T3	T3	T3
Financial Loss -2	T2	T2	T3	T3	T3	T3	T4	T4	T4
Reputation/ Image -3	T1	T1	T2	T2	T2	T3	T3	T4	T4
Unauthorized Release -4	T1	T2	T2	T2	T2	T3	T3	T4	T4
Personal Safety -5	T3	T3	T3	T3	T3	T3	T4	T4	T4
Civil Criminal - 6	T2	T3	T3	T3	T3	T4	T4	T4	T4

T1 = Low Trust
T2 = Medium Trust
T3 = High Trust
T4 = Very High Trust

TMI Reference Model: Example Scenario



TMI Reference Model: Application

- **Identify the assets and providers involved and establish identity, configuration, policy, enforcement authority and reputation compliance, store in the trusted entity store**
- **For each segment of the transaction, identify the level of risk inherent based on the transaction characteristics**
- **Identify mitigation patterns addressing the risks, factoring:**
  - The level of assurance that claims and attestations are valid
  - The level of policy enforcement that can be applied
  - The ability to control rights granted to the transaction principals
- **Assess the overall transaction risk, aligning transaction profile to policy profiles for execution**
- **Audit transaction execution**

TMI Reference Model: Expected Outcomes

- **In an IT commons based on multi-tenant, shared infrastructure, the challenge is to:**
  - Establish trust in the provider of IT services
  - Establish and monitor compliance to changing IT policy
  - Assess and monitor compliance to cost, policy and performance objectives
  - Do this in a multi-sourced, multi-supplier ecosystem
- **To establish and maintain trustworthy ecosystems:**
  - Enable businesses to assess the trustworthiness of supplier systems
  - Enable real-time assessment of compliance as part of the provisioning process
  - Define and implement best practices and standard patterns for building and operating trustworthy infrastructures
  - Define mapping of standards against a reference model to improve integration of trustworthy components
  - Support real time assessment and enforcement of policy to ensure shared infrastructure remains in compliance

The use of open trusted platform standards provides businesses a way to assess the suitability, compliance and performance of shared systems

Questions?