TCG Trusted Multi-Tenant Infrastructure Use Cases

Specification Version 1.0
Revision 1.0
February 14, 2011
TCG Published

Contact: admin@trustedcomputinggroup.org

TCG Published

Copyright © TCG 2011

TCG

Disclaimers, Notices, and License Terms

THIS SPECIFICATION IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE.

Without limitation, TCG disclaims all liability, including liability for infringement of any proprietary rights, relating to use of information in this specification and to the implementation of this specification, and TCG disclaims all liability for cost of procurement of substitute goods or services, lost profits, loss of use, loss of data or any incidental, consequential, direct, indirect, or special damages, whether under contract, tort, warranty or otherwise, arising in any way out of use or reliance upon this specification or any information herein.

This document is copyrighted by Trusted Computing Group (TCG), and no license, express or implied, is granted herein other than as follows: You may not copy or reproduce the document or distribute it to others without written permission from TCG, except that you may freely do so for the purposes of (a) examining or implementing TCG specifications or (b) developing, testing, or promoting information technology standards and best practices, so long as you distribute the document with these disclaimers, notices, and license terms.

Contact the Trusted Computing Group at www.trustedcomputinggroup.org for information on specification licensing through membership agreements.

Any marks and brands contained herein are the property of their respective owners.

Table of Contents

1 Scope and Audience

Thee TCG Trusted Multi-Tenant Infrastructure Use Cases consider a broad range of usage where TCG technology may be applied between components in an enterprise context. They may likewise influence facets of other TCG committees including TPM, TSS, and TC. We anticipate the use cases will be used to derive requirements and prioritize enabling work carried out by the TCG Trusted Multi-Tenant Infrastructure Work Group.

2 TCG Trusted Multi-Tenant Infrastructure Use Cases

The main idea is to map TCG technology and other appropriate industry standards to describe the foundational relationship between the various components in a trusted computing domain and how they interact based on the 3 core functions below. In this process we will identify propose an approach for any gap that exist.

- Establish a Trusted Context
- Exchange Information
- Enforce Policy

With these functional primitives in place, a consumer domain could validate the ability of an environmental provider to enforce separation and operational policy within a cloud or shared infrastructure context. In terms of context – "separation" means that the services, systems and data that comprise a trusted security domain are completely separate from other trusted security domains within the cloud so that only by explicit allowances in operational policy from both trusted security domains can one domain even be aware of another domain. This separation occurs as a logical construct. The scenarios focus on describing the use cases, measurements and validation mechanisms to address the security concerns of enterprise consumers.

2.1 Use Case Categorization

Prior to Bucketing and Prioritization, the Use cases examined by TMI-WG will be divided into three categories:

1. TCG Generic Use Cases. These Use Cases apply to Trusted Platforms or Infrastructures as a whole and are not specific to the purposes of establishing a secure systems domain across multiple infrastructure components capable of enforcing separation of system domains. These Use Cases will be collected, with any analysis and forwarded to the TC for consideration.
2. TCG Multi-Tenant Use Cases. These Use Cases are specific to the purposes of establishing a secure systems domain across multiple infrastructure components capable of enforcing separation of trusted system domains, and should be considered for determining Trusted Multi-Tenant Infrastructure characteristics.
3. TCG Multi-Tenant Use Case Scenarios. These uses cases do not apply generically to all Industries or domains, but may be of interest to Industry or Domain specific specifications.

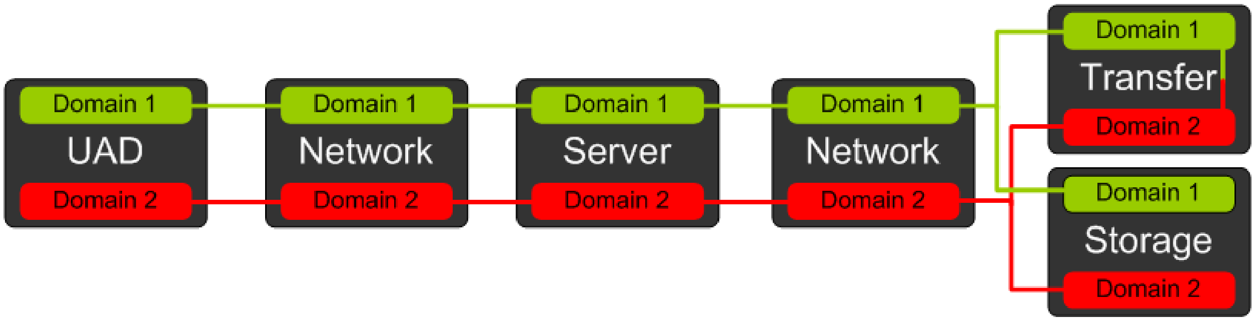
2.2 Use Case vs. Usage Scenario classification

A TMI Use Case is an application of TCG standards in an environment where an "End User" sees benefit to using a TPM based Trusted Environment over an Environment without TPM based Trust Model. A TMI Usage Scenario is a description of a specific instance of a use case. The basic approach is to identify a path though a use case, or through a portion of a use case, and then write the scenario as an instance of that path. Where a use case has several alternate paths, multiple usage scenarios might be written to show how a use case is implemented in practical terms.

2.3 TMI Terminology

In this section we will discuss some of the specific terminology for the TMI Use Cases – some of the terms that are going to be used are industry wide terms that have specific connotations when used in the TMI Use Cases.

In the diagram below is the simplified view of the TMI Reference Architecture and the view of the TMI in terms of multiple domains within a single logical service.



The table below is a list of those most common terms and some contextual information on each of the terms. In most cases the terms are actually "actors" within the use cases.

Term	Definition – Context
Trusted Systems Domain	A logical grouping containing one or more systems governed by a consistent set of operational and security policies
Consumer Domain	A logical grouping containing one or more components available for use by a Consumer and governed by a consistent set of operational and security policies
Provider Domain	A logical grouping containing one or more components available for allocation to a consumer and governed by a consistent set of operational and security policies
Systems Domain	A default domain (containing no policy) that is issued from the Provider to the Consumer for configuration. In short – this domain is "empty" and has not been deployed yet
Policy Enforcement Point	See TNC standard.
Policy Decision Point	See TNC Standard.
Policy Information Point	A repository of Policy Attributes and assertions
Communications Channel	A point-to-point path as defined by both the consumer and provider policy that allows for communications between distinct domains
Trusted Systems	A PDP which contains the default repository of Policy Statements for each Trusted Systems Domain. Owned by

Domain Policy Store	the Trusted Systems Domain.
Provider Systems Domain Policy Store	A PDP which contains the default repository of Policy Statements for each provider. Owned by the Provider
Provider Management Agent	The Systems Management automation suite acting on behalf of a provider organization as a PEP for the provider.
Consumer Management Agent	The Systems Management automation suite acting on behalf of a consumer organization as a PEP for the Trusted Systems Domain
Consumer	The party responsible for the assets within a Trusted Systems Domain
Asset	A functional IT component available for use within a Trusted Systems Domain
Policy	A principle or rule to guide decisions and achieve rational outcome(s)
Provider Environment	A logical grouping containing one or more components available for allocation to a consumer and governed by a consistent set of operational and security policies
Server	A physical or virtual server machine
Storage Volume	A physical or virtual storage container capable of being mounted as a volume on an OS instance
Communications Channel	A physical or virtual communications path between assets in a Trusted Systems Domain.
Data Exchange Gateway	Provides controlled information exchange across the boundary between asset domains. The data exchange gateway is a logical construct that is dictated by both the consumer policy and provider policy that allows for only a set of communications and protocols as dictated by the policies of both the consumer and provider. Responsibility of providing the Data Exchange Gateway is typically on the Provider and the policies of actual communication on the Consumer.
Peripheral Device	A device such as a printer, copier, scanner or other network connected device allocated within a Trusted Systems Domain
Client Device	An external (not a part of the Trusted Systems Domain) end user device that allows the consumer to access the Trusted Systems Domain
Provider Environment Policy	A set of rules that establish a given policy of actions and allowed activity that governs the Provider Environment
Compliant Asset	An asset that has met the pre-determined criteria for use

	within the Trusted Systems Domain
Provider Centralized Audit Collection Environment	Collects audit data from various Assets within the Provider Systems Domain.
Consumer Audit Agent	Requests from the assets logs of their activity within the Trusted Systems Domain. The data require for each asset is controlled by the policy of the Trusted Systems Domain. Owned by the consumer.
Provider Audit Agent	Requests from the assets logs of their activity within the Provider Systems Domain. The data require for each asset is controlled by the policy of the Provider Systems Domain. Owned by the provider.
Consumer Centralized Audit Collection Environment	Collects audit data from various Assets within the Trusted Systems Domain.
Quarantine	The Quarantine holds assets that have become non-compliant. Assets that are quarantined may be able to be provisioned so that they can be returned to service.

2.4 Comparison of Provider and Consumer Use Cases

The following table reflects a comparison of the Provider and Consumer Use Cases – this shows that while independent of one another the Provider will have an effect on the Consumer and vice versa. The key here is to understand that the use case steps do not collide with one another – they will certainly interact with one another but they do not collide or attempt to execute conflicting instructions. There are several scenarios here that deal with change within the consumer domain – these changes are based upon any number of real use case situations such as platform updating due to vendor patches and updates or upgrading of underlying hardware or an increase in compute capacity.

Consumer Management Use Cases			
Consumer UC #	**Provider UC#**	**Description**	**Status**
UC-1 Consumer	No Direct Mapping	Modification of the established Trusted System Domain Policy.	Review
UC-2 Consumer	No Direct Mapping	Use of the Consumer Management Agent to manage resources within the Trusted System Domain	Review
UC-3 Consumer	UC-3 Provider	Use of the Consumer Management Agent after deviation from Trusted Systems Domain steady state after modification of platform	Review

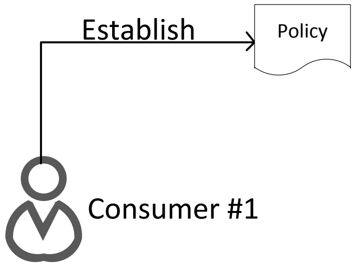
		environment hardware/software.	
UC-4 Consumer	UC-3 Provider	Use of the Provider Management Agent after deviation from Trusted Systems Domain steady state after modification of Platform Environment hardware/software.	Review
UC-5 Consumer	UC-5 Provider	The retirement of the Asset within the Trusted Systems Domain	Review
UC-6 Consumer	UC-6 Provider	Audit of policy within the Trusted Systems Domain.	Review

2.5 Generic Use Cases

This section describes the generic or general use cases that describe the TMI framework. These use cases are not specific to the Provider of a Trusted Systems Domain or a Consumer of those services that a Provider will provide. Each of these use cases can be applied to either one.

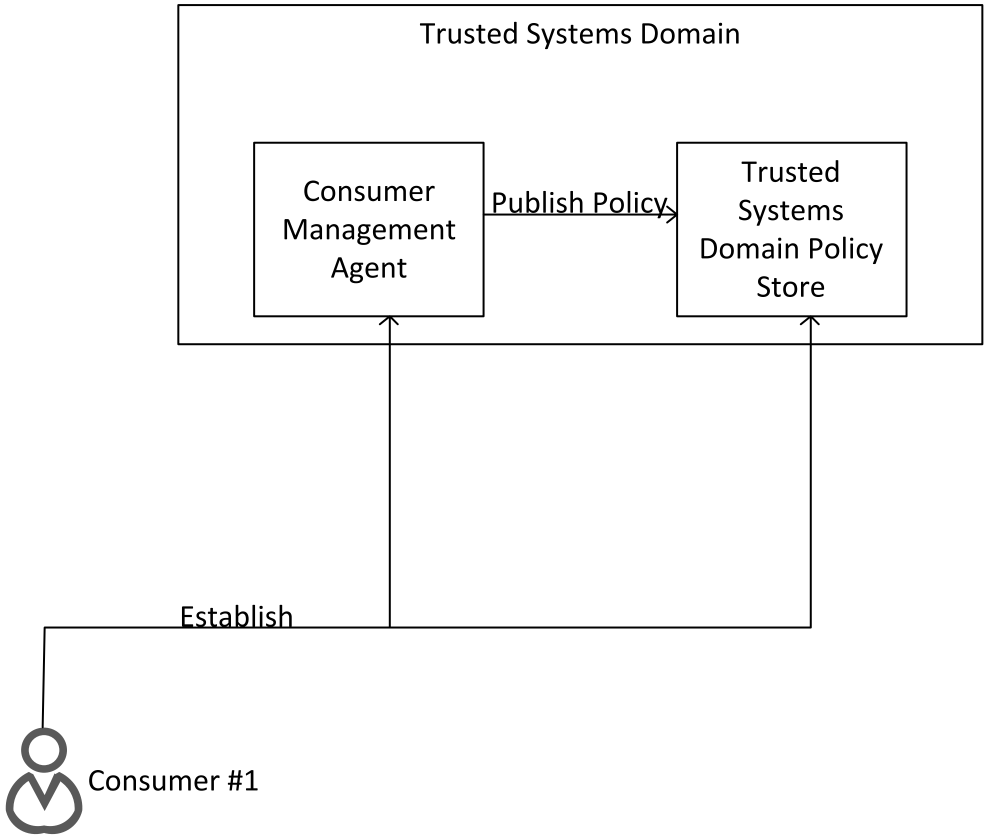
Trusted Systems Domain Provisioning Use Cases				
UC #	**Category**	**Subcategory**	**Description**	**Status**
UC-1 Generic			Establish a Policy	Review
UC-2 Generic			Establish a Trusted Systems Domain	Review
UC-3 Generic			Consumer Management Agent establishes a Trusted System Domain Resource Pool	Review
UC-4 Generic			Provider provisions a server for a consumer within a Trusted Systems Domain	Review
UC-5 Generic			Provision Storage within a Trusted Systems Domain	Review
UC-6 Generic			Provisioning a communications channel between Assets within a Trusted Systems Domain	Review
UC-7 Generic			Provision a Data Exchange Gateway at the Trusted Systems Domain boundary	Review
UC-8 Generic			Provision a peripheral device within the Trusted Systems Domain	Review
UC-9 Generic			Enforce connection policy for a client of the Trusted Systems Domain	Review
UC-10 Generic			Provision application components within the Trusted Systems Domain	Deferred

Ref. #	**Use Case Name**
UC-1 Generic	Establish a Policy
Description	
The main idea is to describe the policies that govern the assets and the interfaces between them assets in a Trusted Systems Domain such that security, performance and availability is maintained	

Actors	
Step #	**Activities**
1	Consumer defines the technical, operational and security control Policy under which the Trusted Systems Domain will operate. This includes the types/quantities of Assets, the Policy for the Assets and relationships between Assets as well as the policy and conditions for separation between the Trusted Systems Domain and other Trusted Systems Domains.
Issues / Key Requirements	
• The use case assumes the following core functional use cases have been defined and are in use: o Establish trust o Exchange Information in a trusted context o Assess and enforce policy statements	
Contributors	
Michael Donovan (HP), Mike Stolp (HP), Erik Visnyak (BAE Systems), Guerney Hunt (IBM)	
Architectural Building Blocks	
	
Threats	
-	

Ref. #	**Use Case Name**
UC-2 Generic	Establish a Trusted Systems Domain
Description	
The main idea is to describe the policies that govern the assets and the interfaces between them assets in a Trusted Systems Domain such that security, performance and availability are maintained configuration.	

Step #	**Activities**
1	Consumer establishes a Trusted Systems Domain Policy Store and Consumer Management Agent for configuration.
2	Consumer Management Agent publishes the Policy to the Trusted Systems Domain Policy Store thus creating the Trusted Systems Domain.
Issues / Key Requirements	
• The use case assumes the following core functional use cases have been defined and are in use: o Establish trust o Exchange Information in a trusted context Assess and enforce policy statements	
o **Contributors**	
Michael Donovan (HP), Mike Stolp (HP), Erik Visnyak (BAE Systems), Guerney Hunt (IBM)	
Architectural Building Blocks	

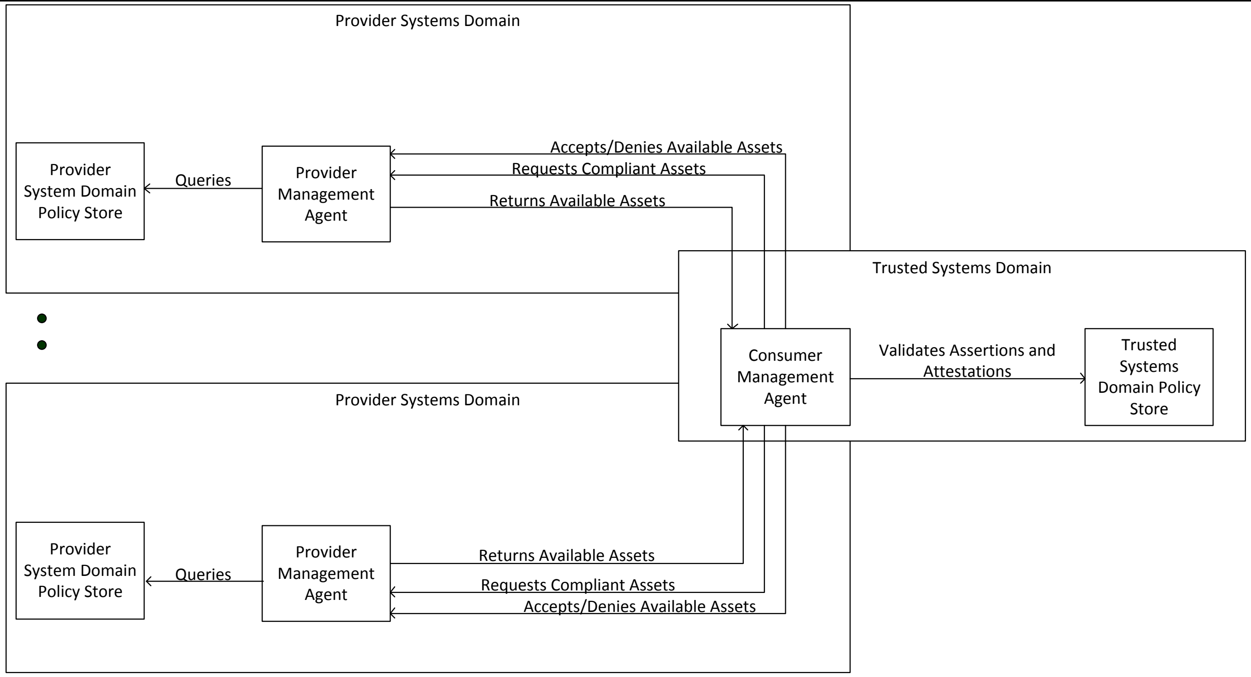

Trusted Systems Domain
Consumer Management Agent
Publish Policy
Trusted Systems Domain Policy Store
Establish
Consumer #1

Threats
-

Ref. #	Use Case Name
UC-3 Generic	Consumer Management Agent establishes a Trusted System Domain Resource Pool

Description
The main idea is to describe the relationship between the various components involved in establishing a secure Trusted Systems Domain and identifying the Provider Environment(s) able to allocate resources to the Trusted Systems Domain in accordance with policy constraints Note the Trusted Systems Domain and Provider Environment may or may not be different organizations but must have some working relationship so the provisioning systems can establish the appropriate level of trust to support the consumer's ability to evaluate the assertions and attestations made by the provider. The Provider Environment must be able to fulfill all of the Consumer Environment policy requirements in the execution of providing services to the Consumer Environment.

Step #	**Activities**
1	The Consumer Management Agent identifies the Environment Providers (internal and external) who will be evaluated for policy compliance to deploy the asset components. CMA can choose to store data about the Providers to be evaluated in the Trusted Systems Domain Policy Store.
2	The Consumer Management Agent queries each Provider Management Agent and determines if the Consumer's Trusted Systems Domain Policy can be met for the types of resources required. Assumption: The Provider Management Agent queries a Provider Systems Domain Policy Store to determine available assets that meet the Consumer's asset request.
3	The Consumer Management Agent confirms whether the assertions and attestations from each Provider Management Agent are compliant with the Consumer's Trusted Systems Domain Policy. The CMA creates a list of trusted providers in the Trusted Domain Policy Store.
4	The Consumer Management Agent may notify each Provider Management Agent that they will or will not be part of the domain resource pool and the types and quantities of Assets needed.
Issues / Key Requirements	
• The use case assumes the following core functional use cases have been defined and are in use: o Establish a Trusted Systems Domain o Establish trust o Exchange Information in a trusted context o Assess and enforce policy statements	
Contributors	
Michael Donovan (HP), Mike Stolp (HP), Erik Visnyak (BAE Systems), Guerney Hunt (IBM)	
Architectural Building Blocks	


Provider Systems Domain
Provider System Domain Policy Store
Queries
Provider Management Agent
Accepts/Denies Available Assets
Requests Compliant Assets
Returns Available Assets
Trusted Systems Domain
Consumer Management Agent
Validates Assertions and Attestations
Trusted Systems Domain Policy Store
Provider Systems Domain
Provider System Domain Policy Store
Queries
Provider Management Agent
Returns Available Assets
Requests Compliant Assets
Accepts/Denies Available Assets

Threats

- The agents must be able to assess the degree of trust in the assertions made (agents could lie)
-

Ref. #	**Use Case Name**
UC-4 Generic	Provisioning a server for a consumer within a Trusted Systems Domain

Description

The main idea is to describe the relationship between the various components involved in the provisioning of a virtual or physical server instance in a providers environment maintaining compliance with the published policies of the Trusted Systems Domain. The physical platform could be shared or dedicated but must appear to be dedicated to the Consumer as part of the Trusted Systems Domain. It is the responsibility of the Consumer to set any sharing constraints as part of the Trusted Systems Domain Policy and the Provider to enforce separation between tenants on a shared server platform.

Step #	**Activities**
1	Consumer Management Agent requests Provider Environment Assets from the Provider Management Agent in the form of a server compliant with the Trusted Systems Domain Policy.
2	The Provider Management Agent allocates server resources for use by the Trusted Systems Domain, transfers control of the server to the Trusted

	Systems Domain, and notifies the Consumer Management Agent that the resources are allocated within the Trusted Systems Domain. Assumption: The Provider Management Agent queries a Provider Systems Domain Policy Store to determine available assets that meet the Consumer's asset request.
3	The Consumer Management Agent validates the provisioned Server against the Trusted Systems Domain Policy Store and accepts/denies the server resources from the Provider Management Agent. If the Consumer Management Agent denies the server resource, control is returned to the Provider Management Agent.

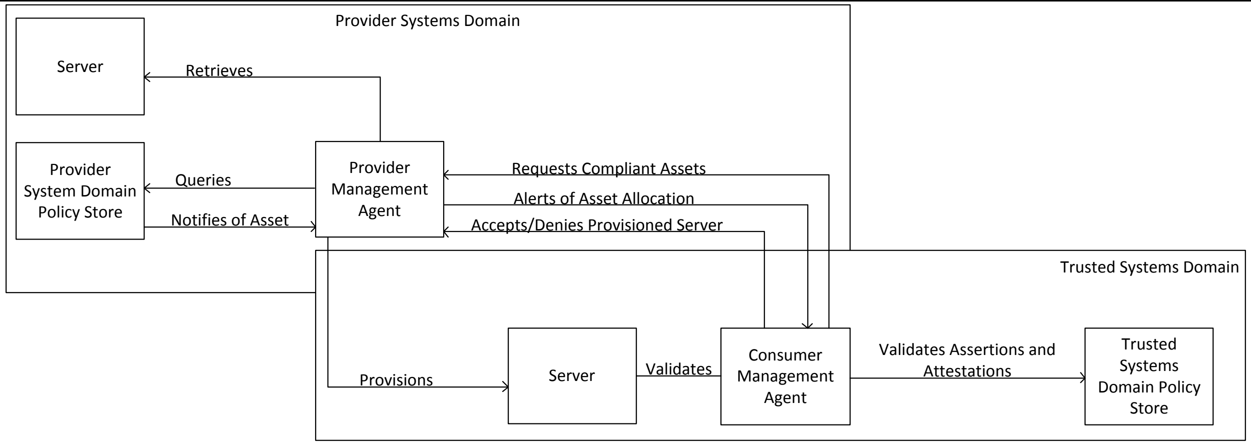
Issues / Key Requirements

- The use case assumes the following core functional use cases have been defined and are in use:
    - Establish a Trusted Systems Domain
    - Establish trust
    - Exchange Information in a trusted context
    - Assess and enforce policy statements
- Servers can be allocated as a) Co-location model where a virtual machine is loaded for execution in a provider environment; b) RAW (no OS), or c) a running machine running the request OS and ready for use. No assumption is made as to whether the underlying hardware is shared or dedicated, only that the degree of separation is equivalent to a dedicated physical machine.

Contributors

Michael Donovan (HP), Mike Stolp (HP), Erik Visnyak (BAE Systems), Guerney Hunt (IBM)

Architectural Building Blocks


Provider Systems Domain
Server
Retrieves
Provider System Domain Policy Store
Queries
Notifies of Asset
Provider Management Agent
Requests Compliant Assets
Alerts of Asset Allocation
Accepts/Denies Provisioned Server
Trusted Systems Domain
Provisions
Server
Validates
Consumer Management Agent
Validates Assertions and Attestations
Trusted Systems Domain Policy Store

Threats

- The consumer agents must be able to assess the degree of trust in the assertions made (provider agents could lie)
- Man in the middle attacks

- Replay attacks
- Trojans, viruses, back doors.

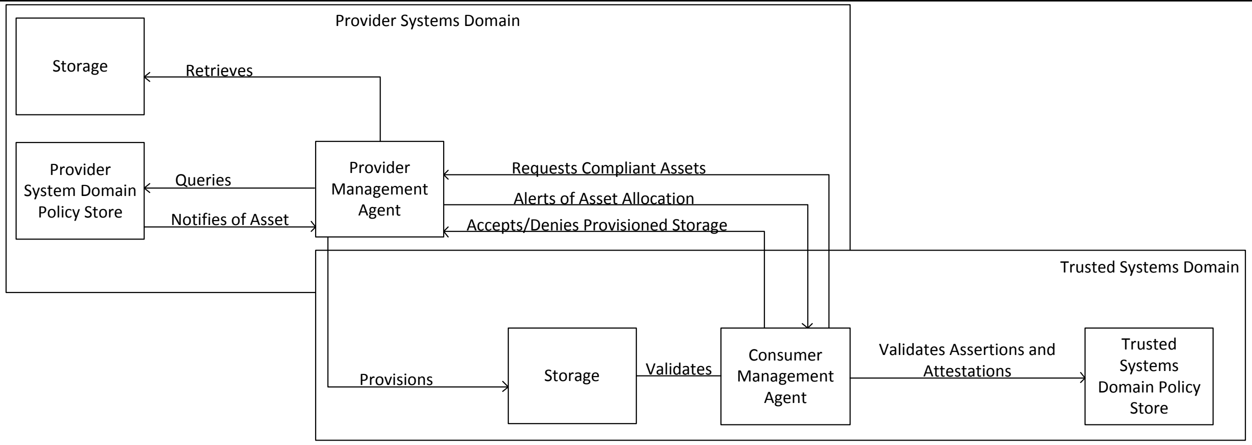
Ref. #	**Use Case Name**
UC-5 Generic	Provisioning Storage within a Trusted Systems Domain
Description	
The main idea is to describe the relationship between the various components involved in the provisioning of a virtual or physical Storage Volume instance in a providers environment maintaining compliance with the published policies of the Trusted Systems Domain. The physical platform could be shared or dedicated but must appear to be dedicated to the Consumer as part of the Trusted Systems Domain. It is the responsibility of the Consumer to set any sharing constraints as part of the Trusted Systems Domain Policy and the Provider to enforce separation between tenants on a shared storage platform.	
Step #	**Activities**
1	Consumer Management Agent requests Provider Environment Assets from the Provider Management Agent in the form of a Storage Volume compliant with the Trusted Systems Domain Policy.
2	The Provider Management Agent allocates storage resources for use by the Trusted Systems Domain; transfers control the Trusted Systems Domain, and notify the Consumer Management Agent that the resources are allocated within the Trusted Systems Domain. Assumption: The Provider Management Agent queries a Provider Systems Domain Policy Store to determine available assets that meet the Consumer's asset request.
3	The Consumer Management Agent validates the provisioned Server against the Trusted Systems Domain Policy Store and accepts/denies the Storage Volume from the Provider Management Agent. If the Consumer Management Agent denies the volume control of the volume is returned to the Provider Management Agent.
Issues / Key Requirements	
• The use case assumes the following core functional use cases have been defined and are in use: o Establish a Trusted Systems Domain o Establish trust o Exchange Information in a trusted context o Assess and enforce policy statements • No assumption is made as to whether the underlying hardware is shared or	

dedicated, only that the degree of separation is equivalent to a dedicated physical storage drive.

Contributors

Michael Donovan (HP), Mike Stolp (HP), Erik Visnyak (BAE Systems), Guerney Hunt (IBM)

Architectural Building Blocks


Provider Systems Domain
Storage
Retrieves
Provider System Domain Policy Store
Queries
Notifies of Asset
Provider Management Agent
Requests Compliant Assets
Alerts of Asset Allocation
Accepts/Denies Provisioned Storage
Trusted Systems Domain
Provisions
Storage
Validates
Consumer Management Agent
Validates Assertions and Attestations
Trusted Systems Domain Policy Store

Threats

- The consumer agents must be able to assess the degree of trust in the assertions made (provider agents could lie)
- Man in the middle attacks
- Replay attacks

Ref. #	Use Case Name
UC-6 Generic	Provisioning a communications channel between Assets within a Trusted Systems Domain

Description

The main idea is to describe the relationship between the various components involved in the provisioning of a Channel (virtual or physical) in a providers environment maintaining compliance with the published policies of the Trusted Systems Domain. The physical platform could be shared or dedicated but must appear to be dedicated to the Consumer as part of the Trusted Systems Domain. It is the responsibility of the Consumer to set any sharing constraints as part of the Trusted Systems Domain Policy and the Provider to enforce separation between tenants on a shared network segment.

Actors

Provider Environment - A logical grouping containing one or more components available for allocation to a consumer and governed by a consistent set of operational and security policies

Provider Systems Domain Policy Store – Default repository of Policy Statements serving as a Policy Information Point (PIP) that can be queried by a Policy Decision

Point (PDP) in response to a challenge from a Policy Enforcement Point (PEP). Issued by the Provider to the Consumer for configuration.

Trusted Systems Domain – A logical grouping containing one or more systems governed by a consistent set of operational and security policies

Trusted Systems Domain Policy Store – A repository of Policy Statements serving as a Policy Information Point (PIP) that can be queried by a Policy Decision Point (PDP) in response to a challenge from a Policy Enforcement Point (PEP)

Provider Management Agent – the Systems Management automation suite acting on behalf of a provider organization

Consumer Management Agent – the Systems Management automation suite acting on behalf of a consumer organization

Communications Channel – A physical or virtual communications path between assets in a Trusted Systems Domain.

Asset – A functional IT component available for use within a Trusted Systems Domain

Policy – a principle or rule to guide decisions and achieve rational outcome(s) [Wikipedia]

Step #	**Activities**
1	Consumer Management Agent requests Provider Environment Assets from the Provider Management Agent in the form of a Communications Channel compliant with the Trusted Systems Domain Policy.
2	The Provider Management Agent allocates network resources for use by the Trusted Systems Domain, Transfers control to the Trusted Systems Domain, and notifies the Consumer Management Agent that the resources are allocated within the Trusted Systems Domain. Assumption: The Provider Management Agent queries a Provider Systems Domain Policy Store to determine available assets that meet the Consumer's asset request.
3	The Consumer Management Agent validates the provisioned Server against the Trusted Systems Domain Policy Store and accepts/denies the Communications Channel from the Provider Management Agent. If the Consumer Management Agent denies the channel, control is returned to the Provider Management Agent.

Issues / Key Requirements

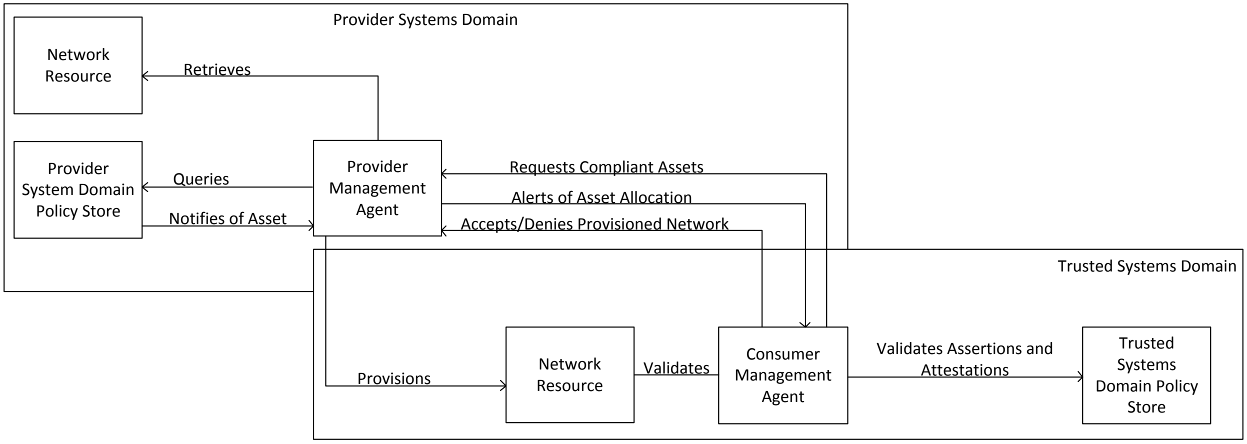
- The use case assumes the following core functional use cases have been defined and are in use:
    - Establish a Trusted Systems Domain
    - Establish trust
    - Exchange Information in a trusted context
    - Assess and enforce policy statements
    - Confirm the attributes of a communications channel.
- The communications channel must be provisioned from asset to asset (e.g. if

between virtual machines on separate physical systems, the channel provision should not terminate at the physical NIC, but at the virtual machine) the consumer must be able to validate where the channel terminates.

Contributors

Michael Donovan (HP), Mike Stolp (HP), Erik Visnyak (BAE Systems), Guerney Hunt (IBM)

Architectural Building Blocks


Provider Systems Domain
Network Resource
Retrieves
Provider System Domain Policy Store
Queries
Notifies of Asset
Provider Management Agent
Requests Compliant Assets
Alerts of Asset Allocation
Accepts/Denies Provisioned Network
Trusted Systems Domain
Provisions
Network Resource
Validates
Consumer Management Agent
Validates Assertions and Attestations
Trusted Systems Domain Policy Store

Threats

- The agents must be able to assess the degree of trust in the assertions made (agents could lie)
- Man in the middle attacks
- Replay attacks

Ref. #	Use Case Name
UC-7 Generic	Provision a Data Exchange Gateway at the Trusted Systems Domain boundary

Description

The main idea is to describe the relationship between the various components involved in the provisioning of a Data Exchange Gateway in a providers environment maintaining compliance with the published policies of the Trusted Systems Domain. The physical platform could be shared or dedicated but must appear to be dedicated to the Consumer as part of the Trusted Systems Domain. It is the responsibility of the Consumer to set any sharing constraints as part of the Trusted Systems Domain Policy.

Step #	Activities
1	Consumer Management Agent requests Provider Environment Assets from the Provider Management Agent in the form of a Data Exchange Gateway compliant with the Trusted Systems Domain Policy.

2	The Provider Management Agent allocates a Data Exchange Gateway (DEG) for use by the Trusted Systems Domain, transfers control of the DEG to the Consumer Management Agent, and notifies the Consumer Management Agent that the DEG are allocated within the Trusted Systems Domain. Assumption: The Provider Management Agent queries a Provider Systems Domain Policy Store to determine available assets that meet the Consumer's asset request.
3	The Consumer Management Agent validates the provisioned Data Exchange Gateway against the Trusted Systems Domain Policy Store and accepts/denies the Data Exchange Gateway from the Provider Management Agent. If the Consumer Management Agent denies the Data Exchange Gateway control of the gateway is returned to the Provider Management Agent.

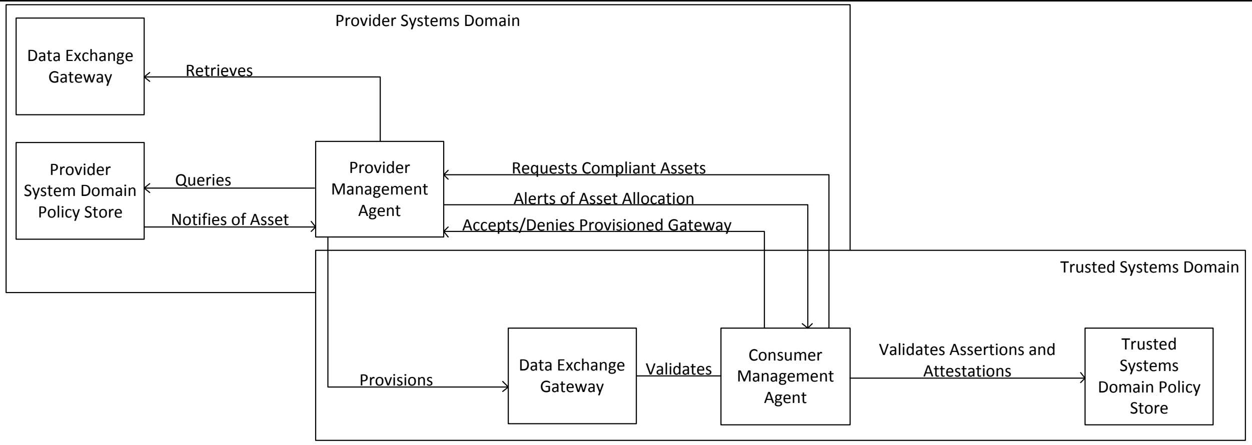
Issues / Key Requirements

- The use case assumes the following core functional use cases have been defined and are in use:
  - Establish a Trusted Systems Domain
  - Establish trust
  - Provisioning a communications channel between Assets within a Trusted Systems Domain
  - Exchange Information in a trusted context
  - Assess and enforce policy statements
- The communications channel must be provisioned from asset to asset (e.g. if between virtual machines on separate physical systems, the channel provision should not terminate at the physical NIC, but at the virtual machine)

Contributors

Michael Donovan (HP), Mike Stolp (HP), Erik Visnyak (BAE Systems), Guerney Hunt (IBM)

Architectural Building Blocks


Provider Systems Domain
Data Exchange Gateway
Retrieves
Provider System Domain Policy Store
Queries
Notifies of Asset
Provider Management Agent
Requests Compliant Assets
Alerts of Asset Allocation
Accepts/Denies Provisioned Gateway
Trusted Systems Domain
Provisions
Data Exchange Gateway
Validates
Consumer Management Agent
Validates Assertions and Attestations
Trusted Systems Domain Policy Store

Threats

- The agents must be able to assess the degree of trust in the assertions made (agents could lie)
- Man in the middle attacks
- Replay attacks

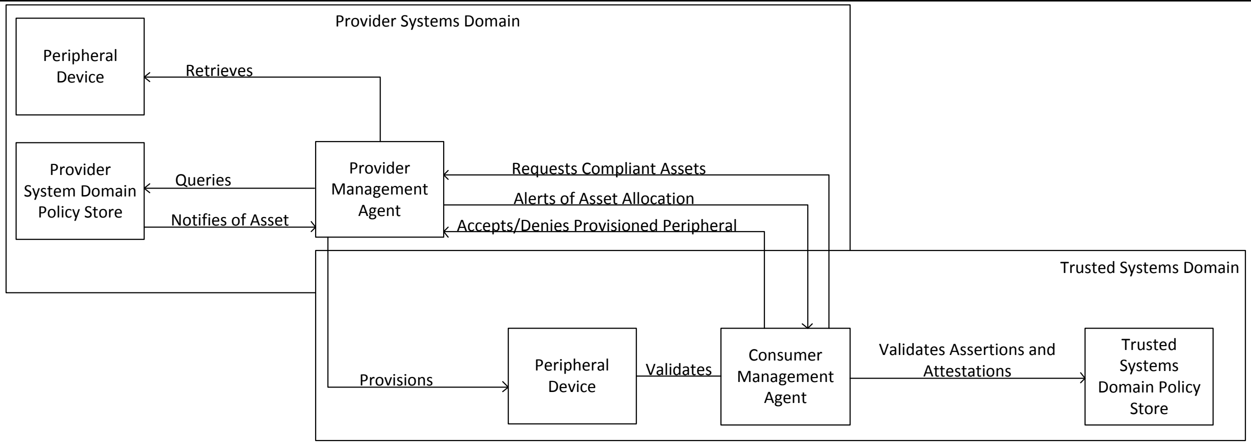
Ref. #	**Use Case Name**
UC-8 Generic	Provision a peripheral device within the Trusted Systems Domain
Description	
The main idea is to describe the relationship between the various components involved in the provisioning of Peripheral Device in a providers environment maintaining compliance with the published policies of the Trusted Systems Domain. The physical platform could be shared or dedicated but must appear to be dedicated to the Consumer as part of the Trusted Systems Domain. It is the responsibility of the Consumer to set any sharing constraints as part of the Trusted Systems Domain Policy and the Provider to enforce separation between tenants using a Peripheral Device.	
Step #	**Activities**
1	Consumer Management Agent requests Provider Environment Assets from the Provider Management Agent in the form of a peripheral device compliant with the Trusted Systems Domain Policy.
2	The Provider Management Agent allocates assets in the form of a peripheral device for use by the Trusted Systems Domain, transfers control of the device to the Trusted Systems Domain, and notifies the Consumer Management Agent that the resources are allocated within the Trusted Systems Domain. Assumption: The Provider Management Agent queries a Provider Systems Domain Policy Store to determine available assets that meet the Consumer's asset request.
3	The Consumer Management Agent validates the provisioned peripheral device against the Trusted Systems Domain Policy Store and accepts/denies the Peripheral Device from the Provider Management Agent and begins using it. If the Consumer Management Agent denies the peripheral device control is returned to the Provider Management Agent.
Issues / Key Requirements	
• The use case assumes the following core functional use cases have been defined and are in use: o Establish a Trusted Systems Domain o Establish trust o Exchange Information in a trusted context o Assess and enforce policy statements	

- The peripheral device may be dedicated or shared, but must appear to the Consumer as a dedicated device.

Contributors

Michael Donovan (HP), Mike Stolp (HP), Erik Visnyak (BAE Systems), Guerney Hunt (IBM)

Architectural Building Blocks


Provider Systems Domain
Peripheral Device
Retrieves
Provider System Domain Policy Store
Queries
Notifies of Asset
Provider Management Agent
Requests Compliant Assets
Alerts of Asset Allocation
Accepts/Denies Provisioned Peripheral
Trusted Systems Domain
Provisions
Peripheral Device
Validates
Consumer Management Agent
Validates Assertions and Attestations
Trusted Systems Domain Policy Store

Threats

- The agents must be able to assess the degree of trust in the assertions made (agents could lie)
- Man in the middle attacks
- Replay attacks
- Man in the middle.

Ref. #	**Use Case Name**
UC-9 Generic	Enforce connection policy for a client of the Trusted Systems Domain

Description

The main idea is to describe the relationship between the various components involved establishing access to assets in the Trusted Computing Domain by a Client Device, maintaining compliance with the published policies of the Trusted Systems Domain. The physical platform could be shared or dedicated but must comply with the Trusted Systems Domain Policy for access to assets and information within the Trusted Systems Domain. It is the responsibility of the Consumer to set any sharing constraints as part of the Trusted Systems Domain Policy and the Provider to enforce separation between tenants using a Client Device.

Step #	**Activities**
1	A Client Device requests access to assets, information or services managed as part of the Trusted Systems Domain.

2	The Consumer Management Agent receives the asset request from the Client Device and forwards the request to the Trusted Systems Domain Policy Store.
4	The Consumer Management Agent notifies the Client Device of acceptance/denial for access to the Asset. If accepted the Client Device accesses the Asset within the Trusted Systems Domain.

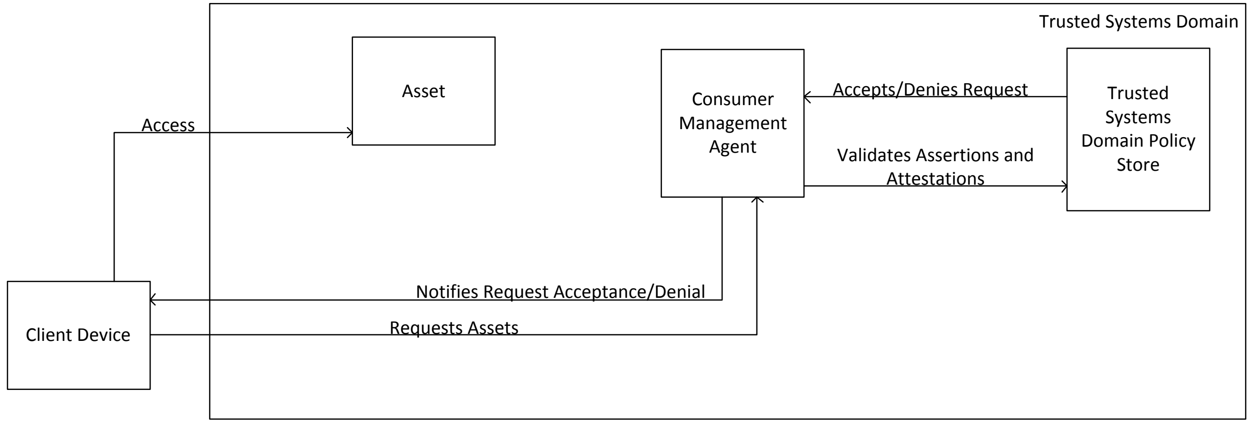
Issues / Key Requirements

- The use case assumes the following core functional use cases have been defined and are in use:
  - Establish a Trusted Systems Domain
  - Establish trust
  - Exchange Information in a trusted context
  - Assess and enforce policy statements
- No assumption is made as to whether the underlying hardware is shared or dedicated, only that the degree of separation is equivalent to a dedicated physical client device.

Contributors

Michael Donovan (HP), Mike Stolp (HP), Erik Visnyak (BAE Systems), Guerney Hunt (IBM)

Architectural Building Blocks


Trusted Systems Domain
Asset
Access
Consumer Management Agent
Accepts/Denies Request
Validates Assertions and Attestations
Trusted Systems Domain Policy Store
Notifies Request Acceptance/Denial
Requests Assets
Client Device

Threats

- The consumer agents must be able to assess the degree of trust in the assertions made (provider agents could lie)
- Man in the middle attacks
- Replay attacks

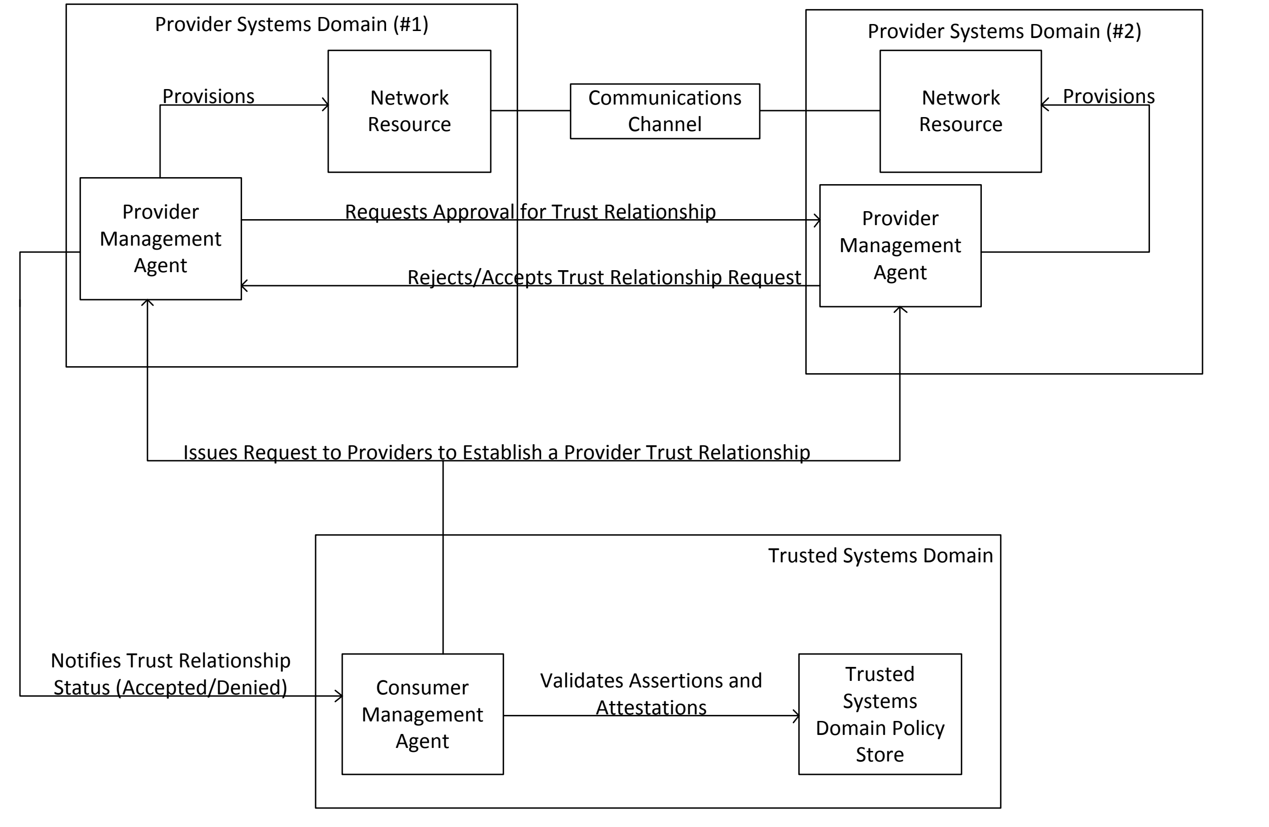
2.6 Provider Use Cases

This section describes the use cases that describe the provider role within the TMI framework.

Provider Management Use Cases				
UC #	**Category**	**Subcategory**	**Description**	**Status**
UC-1 Provider			Establish a trust relationship between Provider Environments.	Review
UC-2 Provider			Modification of the established Provider Environment Policy.	Review
UC-3 Provider			Operation of the surge capability within the Secure System Domain	Review
UC-4 Provider			Transfer Trusted Systems Domain Assets in response to full or partial failure of a Platform Environment.	Review
UC-5 Provider			Re-provision Consumer Assets based on non-compliance.	Review
UC-6 Provider			Audit of policy within the Provider Environment Policy.	Review

Ref. #	**Use Case Name**
UC-1 Provider	Establish a trust relationship between Provider Environments
Description	
The main idea is to describe the establishment of a trust relationship between Provider Environments to enable the exchange of information in support of a trusted systems domain. - Provider Environments exist -Provider Policy has attributes that allow/expect trust to be established	
Step #	**Activities**
1	The Consumer Management Agent may issues a request to the first and second Provider Management Agents to establish Provider to Provider communication in support of the Trusted Systems Domain Or a Provider may choose to establish a provider to provider relationship.
2	The first Provider Management Agent requests approval for the

	establishment of trust relationship the second Provider Management Agent.
3	The second Provider Management Agent rejects/accepts the first Provider Management Agent’s trust request.
4	If the second Provider Management Agent rejects the first Provider Management Agents request then the first Provider Management Agent notifies the Consumer Management Agent for the Trusted Systems domain that are using assets from both providers that Provider to Provider communication will not be supported.
5	If the second Provider Management Agent accepts the first Provider Management Agents trust request then both the first and second Provider Management Agents provision network resources establishing a communication path between the Providers and the first Provider notifies the Consumer Management Agent of the trust relationship. If required by consumer policy.
6	If notified, the Consumer Management Agent validates and attests the new established Provider trust relationship against the Trusted Systems Domain Policy Store.
Issues / Key Requirements	
• The use case assumes the following core functional use cases have been defined and are in use: o Establish a Trusted Systems Domain o Establish trust o Exchange Information in a trusted context o Assess and enforce policy statements o Establish trust between Provider Environments o Exchange Information between those in a trusted context o Assess and enforce policy statements	
Contributors	
Michael Donovan (HP), Mike Stolp (HP), Erik Visnyak (BAE Systems), Guerney Hunt (IBM)	
Architectural Building Blocks	


Provider Systems Domain (#1)
Provider Systems Domain (#2)
Provisions
Network Resource
Communications Channel
Network Resource
Provisions
Provider Management Agent
Requests Approval for Trust Relationship
Provider Management Agent
Rejects/Accepts Trust Relationship Request
Issues Request to Providers to Establish a Provider Trust Relationship
Trusted Systems Domain
Notifies Trust Relationship Status (Accepted/Denied)
Consumer Management Agent
Validates Assertions and Attestations
Trusted Systems Domain Policy Store

Threats
-

Ref. #	**Use Case Name**
UC-2 Provider	Modification of the established Provider Environment Policy

Description
A modification being made to the established Provider Environment Policy - The Consumer must be notified of the impending change in policy

Step #	**Activities**
1	Provider modifies the Provider Systems Domain Policy Store.
2	Provider Management Agent Notifies the Consumer Management Agent when the impending Provider Environment Policy change will take effect.

3	If the Consumer Management Agent accepts the Provider Environment Policy change, the Consumer Management Agent is responsible to make the necessary changes to the Trusted Domain Policy Store for affected Trusted Domains.
4	If the Consumer Management Agent rejects the change, then the Consumer Management Agent is responsible to request that the Provider Management Agent de-provision assets from the Provider environment.

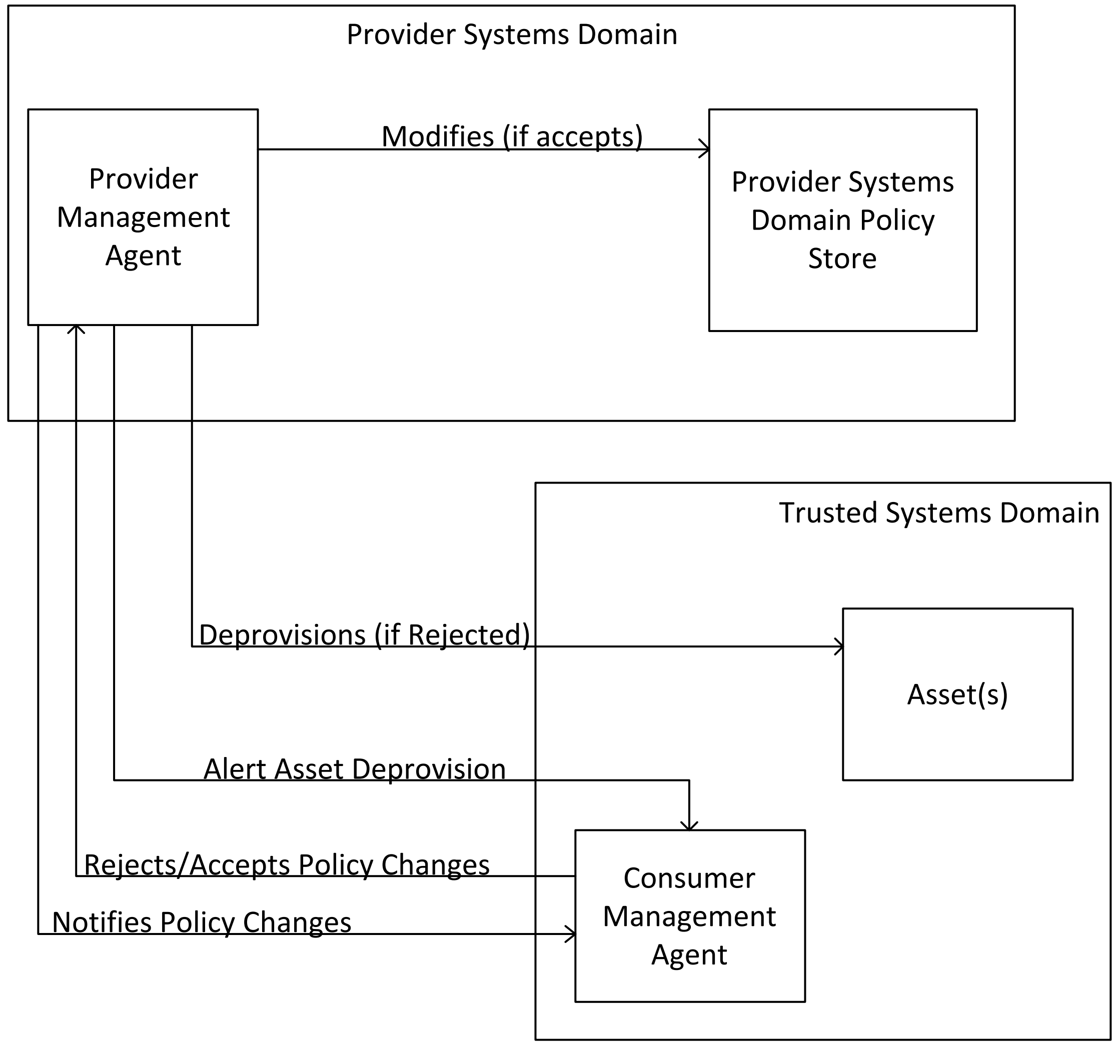
Issues / Key Requirements

- The use case assumes the following core functional use cases have been defined and are in use:
    - Establish a Trusted Systems Domain
    - Establish trust
    - Exchange Information in a trusted context
    - Assess and enforce policy statements
    - Provider policy allows for change to environment
    - Assess and enforce policy statements

Contributors

Michael Donovan (HP), Mike Stolp (HP), Erik Visnyak (BAE Systems), Guerney Hunt (IBM)

Architectural Building Blocks


Provider Systems Domain
Provider Management Agent
Modifies (if accepts)
Provider Systems Domain Policy Store
Trusted Systems Domain
Deprovisions (if Rejected)
Asset(s)
Alert Asset Deprovision
Rejects/Accepts Policy Changes
Notifies Policy Changes
Consumer Management Agent

Threats
-

Ref. #	**Use Case Name**
UC-3 Provider	Operation of the surge capability within the Trusted System Domain
Description	
This use case describes the steps required to operate a Trusted System Domain in a surge capacity where either by Consumer Policy initiation, Policy initiation or other mechanism a given Secure System Domain will be able to garner additional resources needed to continue a given level of service due to additional capacity requirements.	

This use case will have an initial set of steps with additional scenarios attached	
Step #	**Activities**
1	Provider Management Agent receives request from Consumer Management Agent for additional resources for the Trusted Systems Domain
2	Provider Management Agent receives resource request from Consumer Management Agent and validates the request against the Provider Systems Domain Policy Store. Assumption: The Provider Management Agent queries a Provider Systems Domain Policy Store to determine available assets that meet the Consumer's asset request.
3a	The Provider Systems Domain Policy Store accepts/rejects the Consumer's resource request and notifies the Provider Management Agent. If the Provider Management Agent is not able to Provision additional assets to the Trusted Systems Domain to meet the request, the Consumer Management Agent is notified and is responsible to contact another Provider.
3b	If a trusted information exchange agreement exists between the first and a second provider, the first Provider Management Agent can forward the Consumer's asset request to a second Provider Management Agent. The second Provider Management Agent validates against their Provider Systems Domain Policy Store whether they can or cannot support the Consumer's asset request and notifies the original Provider Management Agent. If the asset request is rejected, the second Provider notifies the first Provider which notifies the Consumer Management Agent for Trusted Systems Domain that the asset request is not supported and the Consumer Management Agent is responsible to contact another Provider.
4	If Provider Management Agent identifies available resource compliant with the Trusted Systems Domain Policy, the Provider Management Agent makes available additional resources to the Trusted Systems Domain. If a trusted information exchange agreement exists between the first and second provider, the first Provider Management Agent can transfer the asset request to the second Provider Management Agent. If the second Provider accepts the attest request from the first Provider then second Provider then provisions assets directly to the Trusted Systems Domain.

5	Once assets are provisioned to the Trusted Systems Domain the Provider Management Agent alerts the Consumer Management Agent of the provisioned assets. The Consumer Management Agent validates and attests the new assets against the Trusted Systems Domain Policy Store.

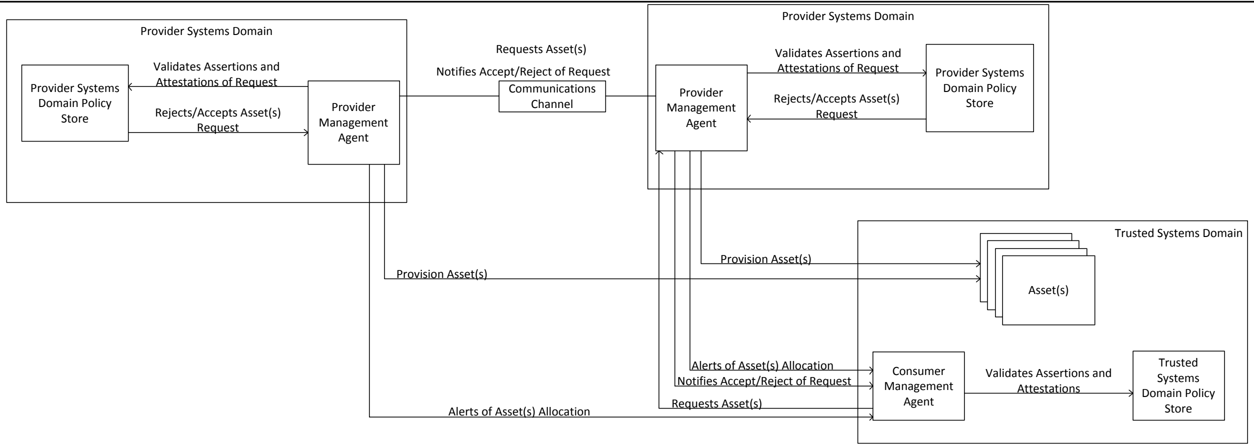
Issues / Key Requirements

- The use case assumes the following core functional use cases have been defined and are in use:
  - Establish a Trusted Systems Domain
  - Establish trust
  - Exchange Information in a trusted context
  - Assess and enforce policy statements
  - Provider policy allows for change to environment
  - Assess and enforce policy statements

Contributors

Michael Donovan (HP), Mike Stolp (HP), Erik Visnyak (BAE Systems), Guerney Hunt (IBM)

Architectural Building Blocks


Provider Systems Domain
Provider Systems Domain Policy Store
Validates Assertions and Attestations of Request
Rejects/Accepts Asset(s) Request
Provider Management Agent
Requests Asset(s)
Notifies Accept/Reject of Request
Communications Channel
Provider Systems Domain
Provider Management Agent
Validates Assertions and Attestations of Request
Rejects/Accepts Asset(s) Request
Provider Systems Domain Policy Store
Trusted Systems Domain
Provision Asset(s)
Provision Asset(s)
Asset(s)
Alerts of Asset(s) Allocation
Notifies Accept/Reject of Request
Requests Asset(s)
Alerts of Asset(s) Allocation
Consumer Management Agent
Validates Assertions and Attestations
Trusted Systems Domain Policy Store

Threats

-

Ref. #	Use Case Name
UC-4 Provider	Transfer Trusted Systems Domain Assets in response to full or partial failure of a Platform Environment.

Description

The main idea is to describe the ability to provide fail over in the event of assets becoming un-available.

Note the Consumer Domain and Provider Environment may or may not be different organizations but must have some working relationship so the VM provisioning systems can establish the appropriate level of trust to support the consumer’s ability to evaluate the assertions and attestations made by the provider.

Step #	**Activities**
2	If the Provider Management Agent is available, then the Provider Management Agent notifies the Consumer Management Agent of the failure.
2a	The Provider Management Agent queries the Provider Systems Domain Policy Store to identify if it has additional compliant assets for the Consumer. If compliant assets are not available to allocate to the Trusted Systems Domain, the Provider Management Agent notifies the Consumer Management Agent. If the consumer’s policy allows it, new assets can be provisioned without notification to the consumer.
2b	However – If a trusted relationship exists between two Providers that allows for the transfer of Consumer’s assets then First Provider Management Agent issues a request to the Second Provider if they can house the Consumer’s assets. The Second Provider Management Agent validates against their Provider Systems Domain Policy Store if the request is supported and notifies its Provider Management Agent which issues an acceptance or denial of control of the Consumer’s assets to the first Provider Management Agent. Assumption Consumer policy allows transfer.
3	If the Consumer Management Agent detects the outage and cannot contact the Provider Management Agent, the Consumer Management Agent may provision Trusted Systems Domain Assets with another Provider.
4	When the first Provider Management Agent comes back online after an outage, it notifies the Consumer Management Agent of a revert back to the original state. Then the second Provider migrates the Consumer’s assets back to the first Provider and both notify the Consumer Management Agent of the migration of assets. Assumption: Automatic return of assets to the original provider cannot be done unless the consumer’s policy allows it. As before migration cannot occur unless there is a secure channel.

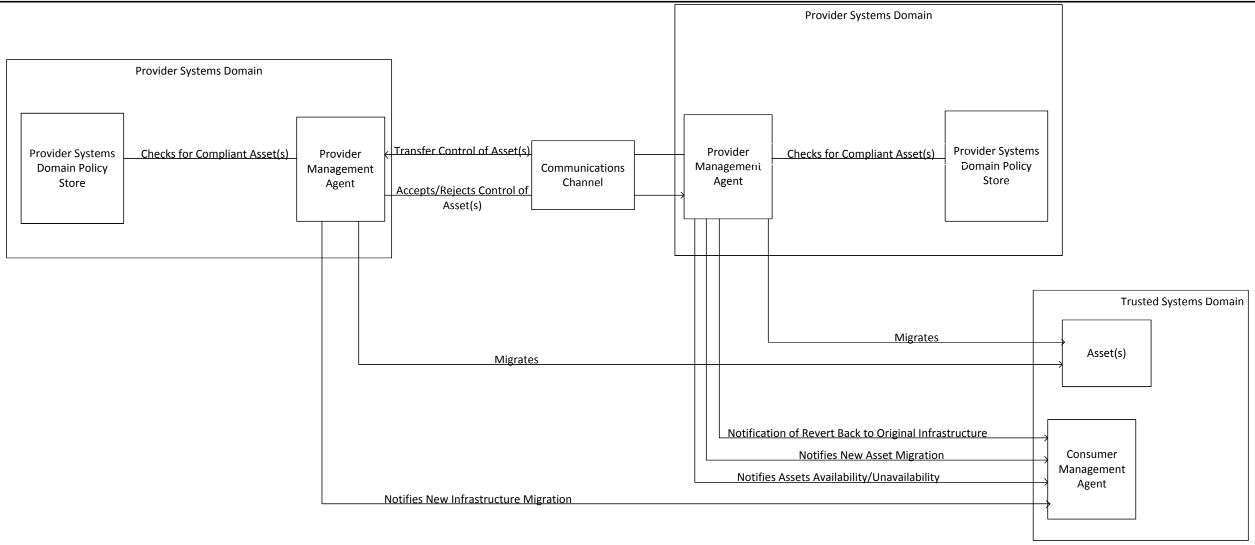
Issues / Key Requirements

- The use case assumes the following core functional use cases have been defined and are in use:
  - Establish a Trusted Systems Domain
  - Establish trust
  - Exchange Information in a trusted context
  - Assess and enforce policy statements
  - Provider policy allows for change to environment
  - Assess and enforce policy statements
- Need to provide scenarios that illustrate the types of policies that might be important in a TMI context
- Assumes provider management agent is available

Contributors

Michael Donovan (HP), Mike Stolp (HP), Erik Visnyak (BAE Systems), Guerney Hunt (IBM)

Architectural Building Blocks


Provider Systems Domain
Provider Systems Domain Policy Store
Checks for Compliant Asset(s)
Provider Management Agent
Transfer Control of Asset(s)
Accepts/Rejects Control of Asset(s)
Communications Channel
Provider Systems Domain
Provider Management Agent
Checks for Compliant Asset(s)
Provider Systems Domain Policy Store
Trusted Systems Domain
Migrates
Asset(s)
Migrates
Notification of Revert Back to Original Infrastructure
Notifies New Asset Migration
Notifies Assets Availability/Unavailability
Notifies New Infrastructure Migration
Consumer Management Agent

Threats

- The agents must be able to assess the degree of trust in the assertions made (agents could lie)
- Man in the middle attacks
- Replay attacks

Ref. #	Use Case Name
UC-5 Provider	Re-provision Trusted Systems Domain Assets based on changes to the Trusted Systems Domain Policy

Description

The main idea is to describe the ability to re-provision Trusted Systems Domain assets based on Trusted System Domain Policy.

Note the Consumer Domain and Provider Environment may or may not be different organizations but must have some working relationship so the VM provisioning systems can establish the appropriate level of trust to support the consumer's ability to evaluate the assertions and attestations made by the provider.

Step #	**Activities**
1	The Consumer Management Agent modifies the Trusted Systems Domain Policy Store. The Trusted Domain Policy Store notifies the Consumer Management Agent that there are now non-compliant Assets within the Trusted System Domain. The Consumer Management Agent notifies the Provider Management of the Trusted Systems Domain Policy Store modifications. The Consumer Management Agent request de-provisioning of the noncompliant assets, returning control of the assets to the Provider Management Agent.
2	If Assets are available, the Provider Management Agent provisions attests to the Trusted Systems Domain, transfers control of the assets to the Consumer Management Agent, and notifies the Consumer Management Agent of the new provisioned assets. The Consumer Management Agent validates and attests the new assets against the Trusted Systems Domain Policy Store. If the assets are rejected, control of the assets is returned to the Provider Management Agent
3	If assets are not available, the Provider Management Agent notifies the Consumer Management Agent that no compliant assets are available.

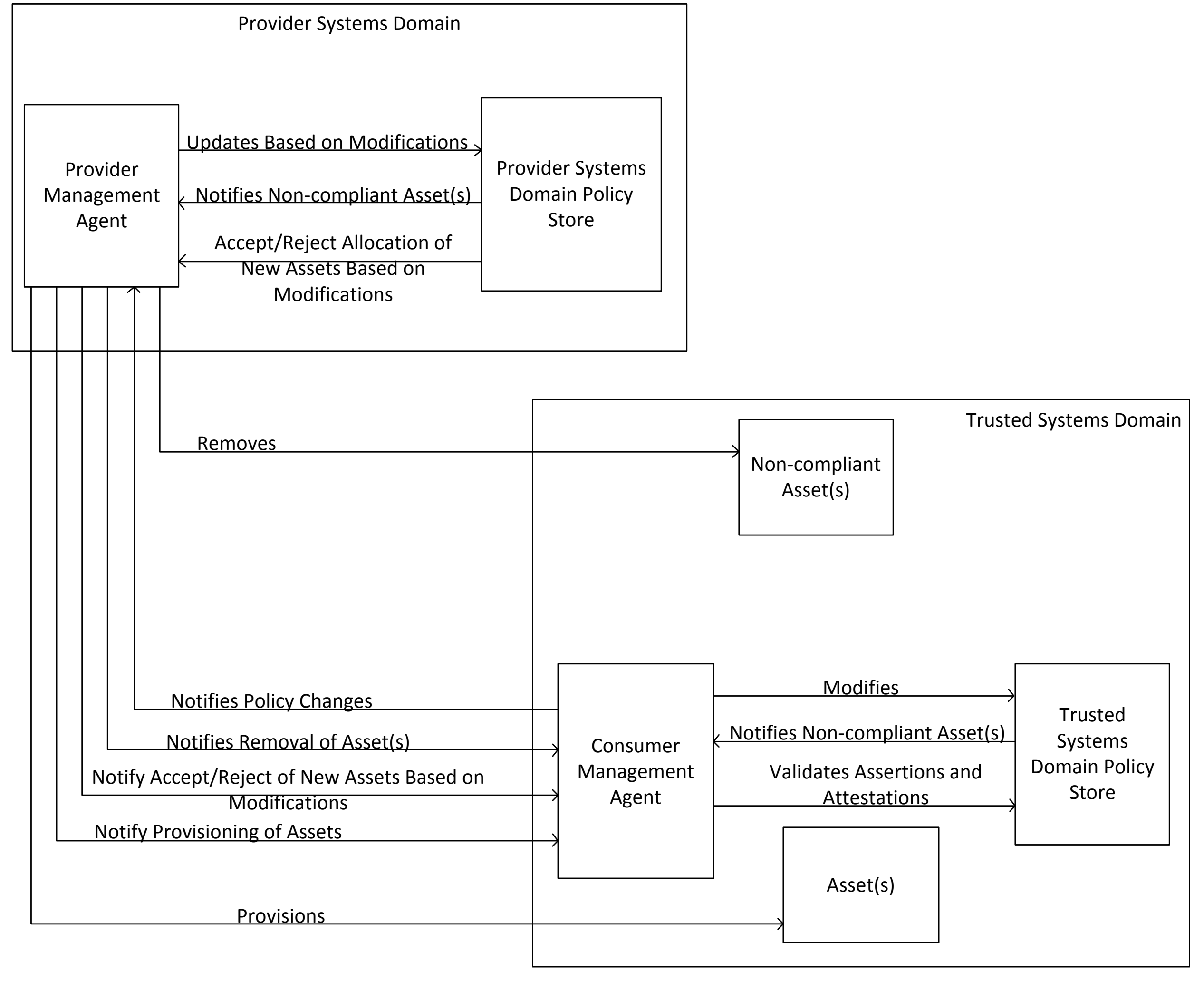
Issues / Key Requirements

- The use case assumes the following core functional use cases have been defined and are in use:
    - Establish a Trusted Systems Domain
    - Establish trust
    - Exchange Information in a trusted context
    - Assess and enforce policy statements
    - Provider policy allows for change to environment
    - Assess and enforce policy statements
- Need to provide scenarios that illustrate the types of policies that might be important in a TMI context

Contributors

Michael Donovan (HP), Mike Stolp (HP), Erik Visnyak (BAE Systems), Guerney Hunt (IBM)

Architectural Building Blocks


Provider Systems Domain
Provider Management Agent
Updates Based on Modifications
Notifies Non-compliant Asset(s)
Accept/Reject Allocation of New Assets Based on Modifications
Provider Systems Domain Policy Store
Trusted Systems Domain
Removes
Non-compliant Asset(s)
Notifies Policy Changes
Notifies Removal of Asset(s)
Notify Accept/Reject of New Assets Based on Modifications
Notify Provisioning of Assets
Provisions
Consumer Management Agent
Modifies
Notifies Non-compliant Asset(s)
Validates Assertions and Attestations
Trusted Systems Domain Policy Store
Asset(s)

Threats
- The agents must be able to assess the degree of trust in the assertions made (agents could lie) - Man in the middle attacks - Replay attacks

Ref. #	**Use Case Name**
UC-6 Provider	Audit of policy within the Provider Environment Policy.
Description	
The main idea is to describe the ability to provide traceability of policy activities within the Provider Environment Policy providing an audit capability to detect compliant and noncompliant activities. Note the Consumer Domain and Provider Environment may or may not be different	

organizations but must have some working relationship so the VM provisioning systems can establish the appropriate level of trust to support the consumer's ability to evaluate the assertions and attestations made by the provider.

Step #	Activities
1	Provider Management Agents make operational requests within the Environment that are forwarded to the Provider Audit Agent.
2	The Provider Audit Agent evaluates the Provider Management Agents operational request and audits activity of Assets to the Provider Environment Policy that is defined within the Provider Domain Policy Store.
3	The Provider Audit Agent alerts designated (controlled by provider policy) Provider Management Agents of critical audit conformance and non-conformance events.

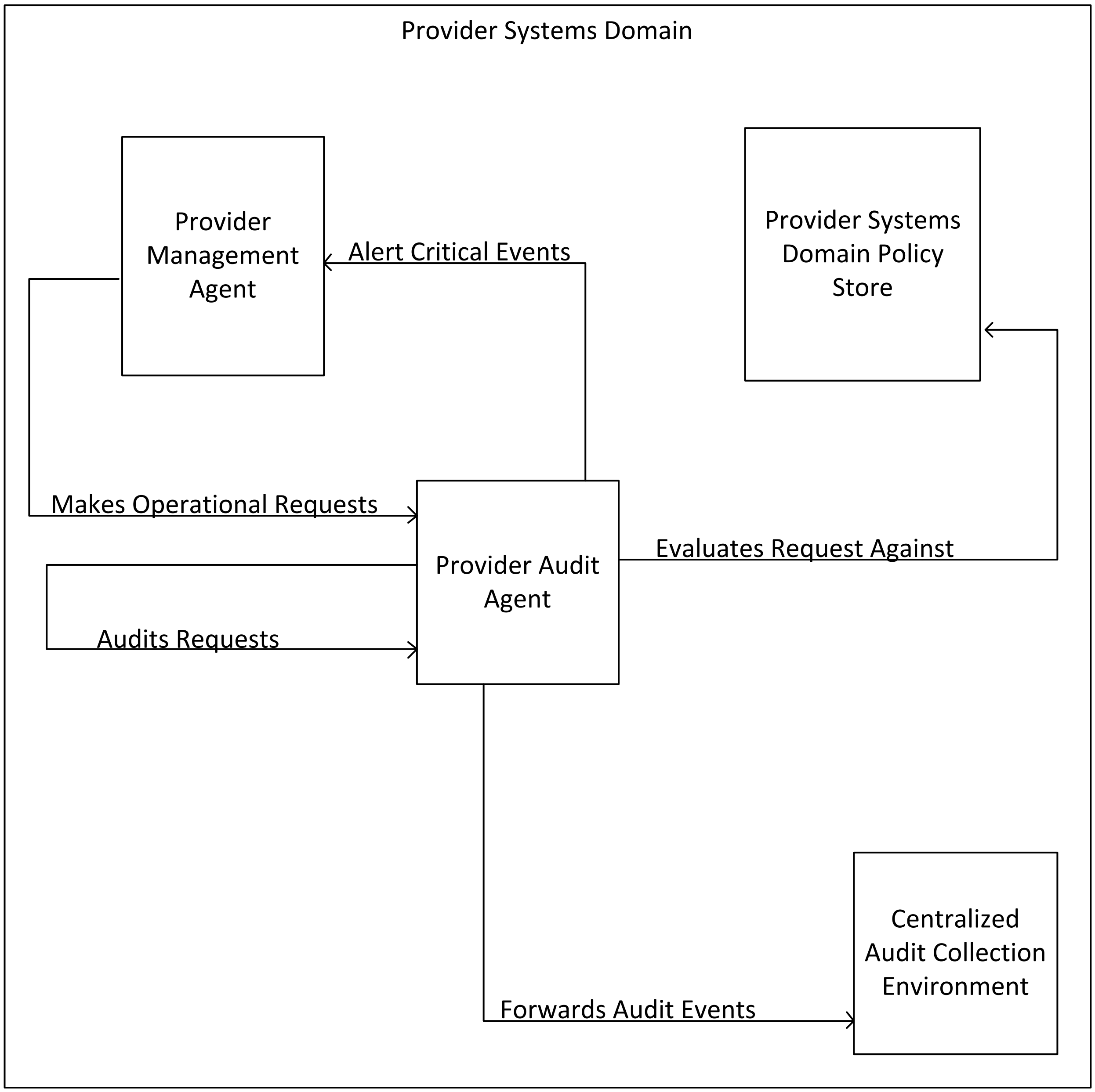
Issues / Key Requirements

- The use case assumes the following core functional use cases have been defined and are in use:
  - Establish a Trusted Systems Domain
  - Establish trust
  - Exchange Information in a trusted context
  - Assess and enforce policy statements
  - Provider policy allows for change to environment
  - Assess and enforce policy statements
- Need to provide scenarios that illustrate the types of policies that might be important in a TMI context
- Assumption – The measurement method and execution of those methods are performed in a manner which can be trusted – so each step of the measurement process can attest to integrity
- Assumption – The storage method of the measurement data is conducted in such a way that the data is secure and maintains integrity. In short – all aspects of the storage, retrieval and access to the stored measurement data (audit data) is executed in such a manner that integrity is assured

Contributors

Michael Donovan (HP), Mike Stolp (HP), Erik Visnyak (BAE Systems), Guerney Hunt (IBM)

Architectural Building Blocks


Provider Systems Domain
Provider Management Agent
Alert Critical Events
Provider Systems Domain Policy Store
Makes Operational Requests
Provider Audit Agent
Evaluates Request Against
Audits Requests
Centralized Audit Collection Environment
Forwards Audit Events

Threats

- The agents must be able to assess the degree of trust in the assertions made (agents could lie)
- Man in the middle attacks
- Replay attacks

2.7 Consumer Use Cases

This section describes the use cases that describe the consumer role within the TMI framework.

Consumer Management Use Cases				
UC #	**Category**	**Subcategory**	**Description**	**Status**
US-1 Consumer			Modification of the established Trusted System Domain Policy.	Review
UC-2 Consumer			Use of the Consumer Management Agent to manage resources within the Trusted System Domain	Review
UC-3 Consumer			Use of the Consumer Management Agent after deviation from Trusted Systems Domain steady state after modification of Platform Environment hardware/software.	Review
UC-4 Consumer			Use of the Provider Management Agent after deviation from Trusted Systems Domain steady state after modification of Platform Environment hardware/software.	Review
UC-5 Consumer			The retirement of the Asset within the Trusted Systems Domain	Review
UC-6 Consumer			Audit of policy within the Trusted Systems Domain.	Review

Ref. #	**Use Case Name**
UC-1 Consumer	Modification of the established Trusted System Domain Policy
Description	
The main idea is to describe the modification of an established Trusted Systems Domain Policy.	

Step #	Activities
1	Consumer Management Agent modifies the Trusted Systems Domain Policy Store.
2	Consumer Management Agent requests approval for the modifications to the Provider Management Agent(s).
3	The Provider Management Agent validates the Consumer's policy changes against the Provider Systems Domain Policy Store and rejects/accepts the Consumer's policy modifications.
4	If the Provider Management Agent rejects the Consumer Management Agent's request then the Consumer Management Agent must either reconfigure/revert back their Trusted Systems Domain Policy Store configuration or request de-provisioning of the Trusted Systems Domain.

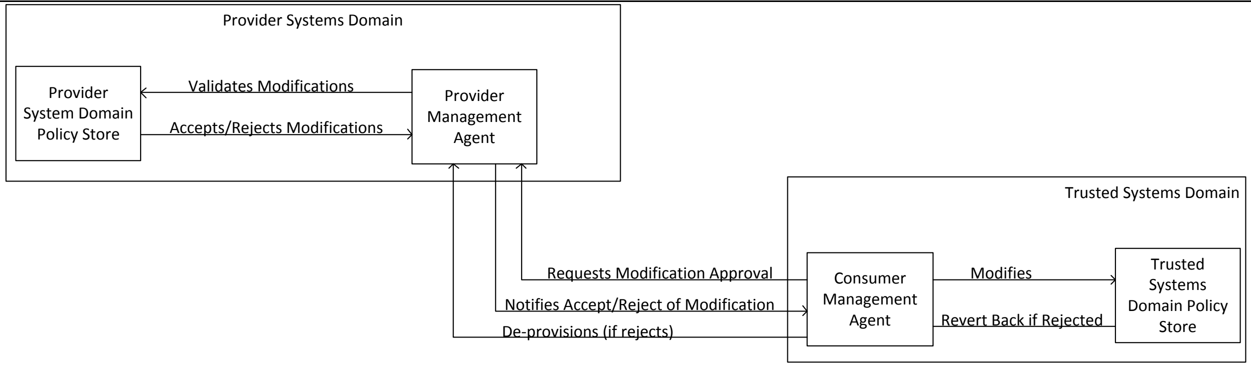
Issues / Key Requirements

- The use case assumes the following core functional use cases have been defined and are in use:
  - Establish a Trusted Systems Domain
  - Establish trust
  - Exchange Information in a trusted context
  - Assess and enforce policy statements
  - Provider policy allows for change to environment
  - Assess and enforce policy statements

Contributors

Michael Donovan (HP), Mike Stolp (HP), Erik Visnyak (BAE Systems), Guerney Hunt (IBM)

Architectural Building Blocks

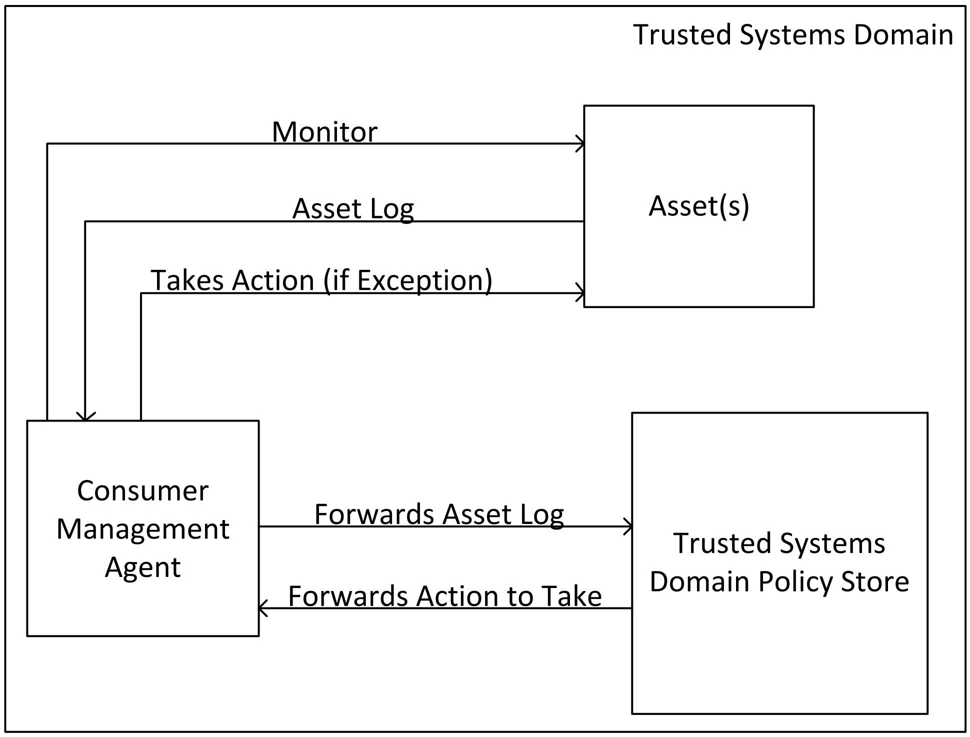

Provider Systems Domain
Provider System Domain Policy Store
Validates Modifications
Accepts/Rejects Modifications
Provider Management Agent
Trusted Systems Domain
Requests Modification Approval
Notifies Accept/Reject of Modification
De-provisions (if rejects)
Consumer Management Agent
Modifies
Revert Back if Rejected
Trusted Systems Domain Policy Store

Threats

-

Ref. #	Use Case Name

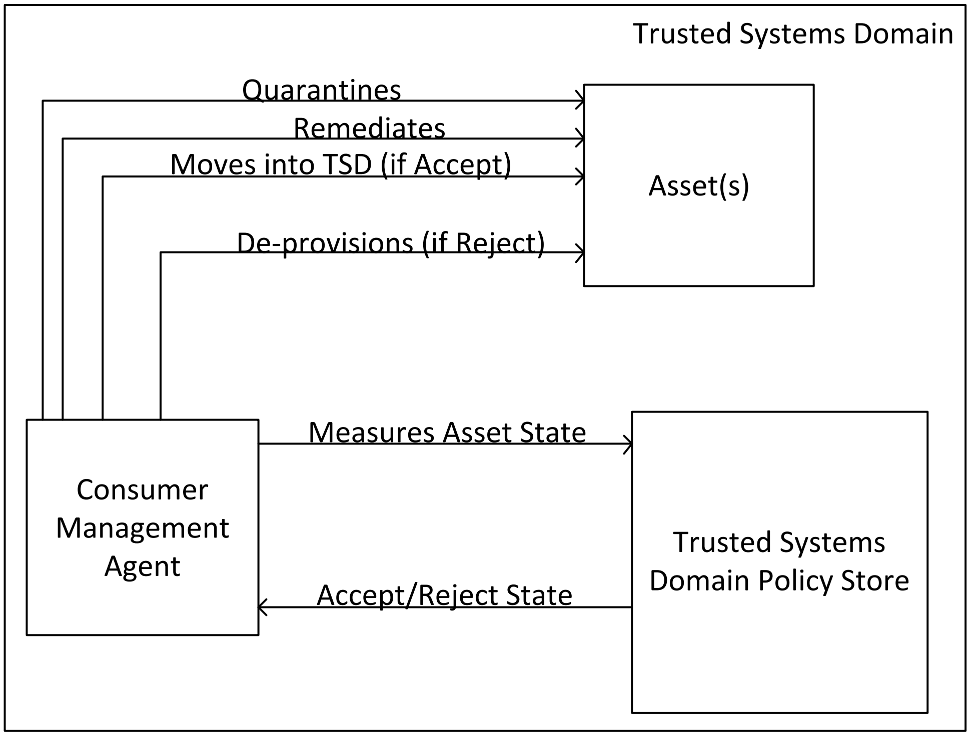
UC-2 Consumer	Use of the Consumer Management Agent to monitor resources within the Trusted System Domain.
Description This use case describes how the Consumer Management Agent monitors assets within the Trusted Systems Domain.	
Step #	**Activities**
1	The Consumer Management Agent interacts with assets within the Trusted Systems Domain to perform monitoring of assets.
2	The Consumer Management Agent request an activity (based on policy) log from an asset. The Consumer Management Agent forwards the log to the Trusted Systems Domain Policy Store to determine if the activity is permitted within the Trusted Systems Domain.
3	The Consumer Management Agent enforces the Trusted Systems Domain Policy Stores decision and takes action (determined by policy) if the asset has performed a non-compliant action.
Issues / Key Requirements	
• The use case assumes the following core functional use cases have been defined and are in use: o Establish a Trusted Systems Domain o Establish trust o Exchange Information in a trusted context o Assess and enforce policy statements o Provider policy allows for change to environment o Assess and enforce policy statements	
Contributors	
Michael Donovan (HP), Mike Stolp (HP), Erik Visnyak (BAE Systems), Guerney Hunt (IBM)	
Architectural Building Blocks	


Trusted Systems Domain
Monitor
Asset(s)
Asset Log
Takes Action (if Exception)
Consumer Management Agent
Forwards Asset Log
Trusted Systems Domain Policy Store
Forwards Action to Take

Threats
-

<table>
<tr><th><b>Ref. #</b></th><th colspan="2"><b>Use Case Name</b></th></tr>
<tr><td>UC-3
Consumer</td><td colspan="2">Use of the Consumer Management Agent after deviation from Trusted Systems Domain steady state after modification of Platform Environment hardware/software.</td></tr>
<tr><td colspan="3"><b>Description</b> How the Consumer Management Agent responds when it detect that assets have become noncompliant to its policy.</td></tr>
<tr><td colspan="3"></td></tr>
<tr><td colspan="3"></td></tr>
<tr><td><b>Step #</b></td><td colspan="2"><b>Activities</b></td></tr>
<tr><td>2</td><td colspan="2">The Trusted Systems Domain Policy Store accepts/denies the state of assets within the Trusted Systems Domain and forwards decisions to the Consumer Management Agent.</td></tr>
<tr><td>3</td><td colspan="2">If an asset state is denied by the Trusted Systems Domain Policy Store then the Consumer Management Agent quarantines the non-compliant asset.</td></tr>
</table>

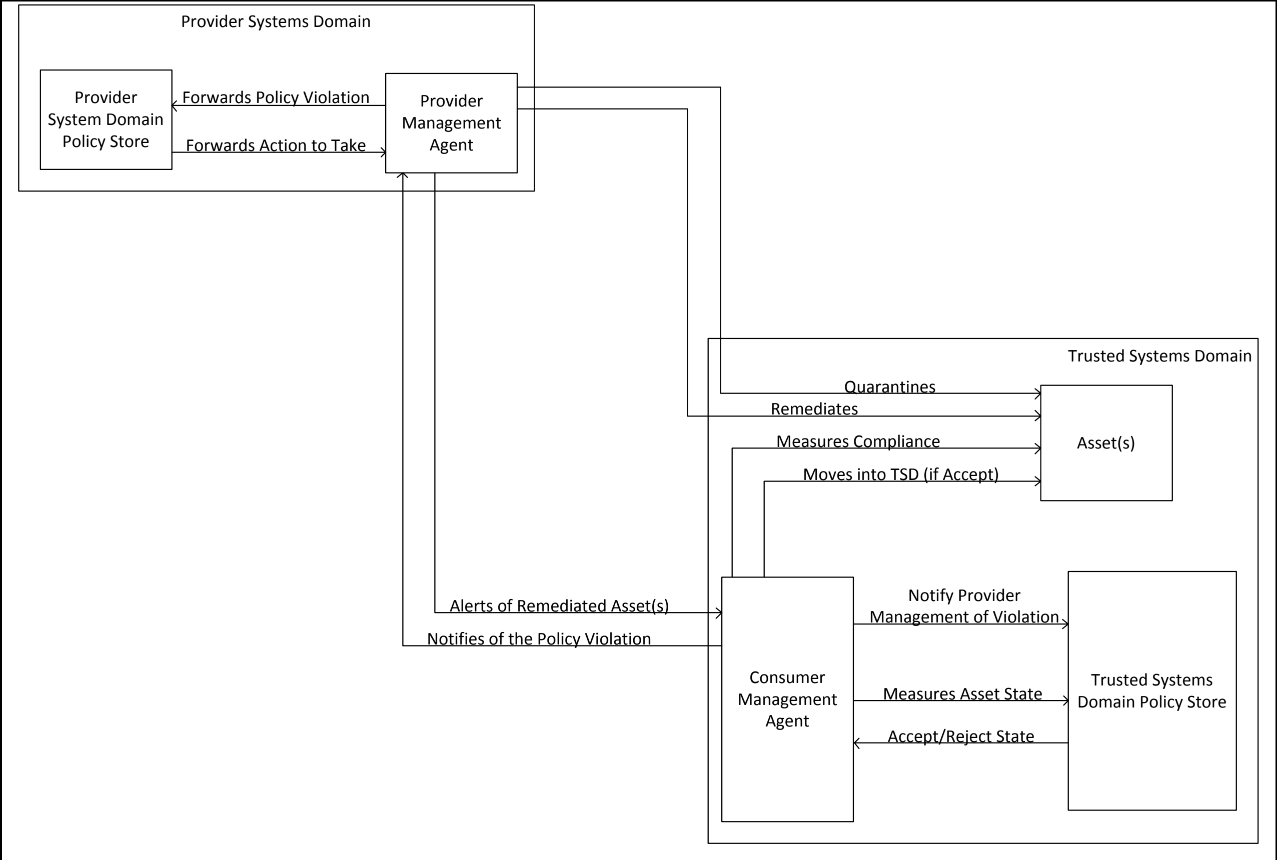
4	The Consumer Management Agent remediates quarantined non-compliant assets.
5	Remediated quarantined assets request access to the Trusted Systems Domain via the Consumer Management Agent.
6	The Consumer Management Agent forwards the assets request and current state to the Trusted Systems Domain Policy Store which accepts/denies the assets ability to move back into the Trusted Systems Domain.
7	If accepted the Consumer Management Agent reallocates the asset back into the Trusted Systems Domain. If rejected then Consumer management agent either request de-provisioning of the asset or quarantines the asset for further remediation. Return of assets that fail remediation will be driven by policy.
Issues / Key Requirements	
• The use case assumes the following core functional use cases have been defined and are in use: o Establish a Trusted Systems Domain o Establish trust o Exchange Information in a trusted context o Assess and enforce policy statements o Provider policy allows for change to environment o Assess and enforce policy statements	
Contributors	
Michael Donovan (HP), Mike Stolp (HP), Erik Visnyak (BAE Systems), Guerney Hunt (IBM)	
Architectural Building Blocks	


Trusted Systems Domain
Quarantines
Remediates
Moves into TSD (if Accept)
De-provisions (if Reject)
Asset(s)
Measures Asset State
Consumer Management Agent
Trusted Systems Domain Policy Store
Accept/Reject State

Threats
-

Ref. #	**Use Case Name**
UC-4 Consumer	Use of the Provider Management Agent after deviation from Trusted Systems Domain steady state after modification of Platform Environment hardware/software.
Description	
The consumer Management Agent detects that that an asset is not in compliance with its policy and request that the Provider Management Agent remediate the asset.	
Step #	**Activities**
1	The Consumer Management Agent detects changes within an asset that are in violation of the Trusted Systems Domain Policy.
2	The Consumer Management Agent notifies the Provider Management Agent of the violation. The Provider Management Agent confirms the policy violation with the Provider Systems Domain Policy Store.
3	If confirmed, the Provider Management Agent quarantines non-compliant hardware/software assets. If the violation is not confirmed the Provider

	Management Agent negotiates the disposition of the asset based on policy with the Consumer Management Agent.
5	The Consumer Management Agent forwards the assets request to the Trusted Systems Domain Policy Store which accepts/denies the assets ability to move back into the Trusted Systems Domain.
6	If accepted the Consumer Management Agent reallocates the asset back into the Trusted Systems Domain. If rejected then Consumer Management Agent either request de-provisioning of the asset or reissues quarantine requests the Provider Management Agent. This action is controlled by the policy of the Trusted System Domain.
Issues / Key Requirements	
• The use case assumes the following core functional use cases have been defined and are in use: o Establish a Trusted Systems Domain o Establish trust o Exchange Information in a trusted context o Assess and enforce policy statements o Provider policy allows for change to environment o Assess and enforce policy statements	
Contributors	
Michael Donovan (HP), Mike Stolp (HP), Erik Visnyak (BAE Systems), Guerney Hunt (IBM)	
Architectural Building Blocks	

<table>
<tr><td>
Provider Systems Domain
Provider System Domain Policy Store
Forwards Policy Violation
Forwards Action to Take
Provider Management Agent
Trusted Systems Domain
Quarantines
Remediates
Measures Compliance
Moves into TSD (if Accept)
Asset(s)
Alerts of Remediated Asset(s)
Notifies of the Policy Violation
Notify Provider Management of Violation
Consumer Management Agent
Measures Asset State
Accept/Reject State
Trusted Systems Domain Policy Store

</td></tr>
<tr><td><b>Threats</b></td></tr>
<tr><td>-</td></tr>
</table>

<table>
<tr><td><b>Ref. #</b></td><td><b>Use Case Name</b></td></tr>
<tr><td>UC-5 Consumer</td><td>The retirement of the Asset within the Trusted Systems Domain</td></tr>
<tr><td colspan="2"><b>Description</b></td></tr>
<tr><td colspan="2">The main idea is to describe the ability to remove an asset from within the Trusted Systems Domain.
Note the Consumer Domain and Provider Environment may or may not be different organizations but must have some working relationship so the VM provisioning systems can establish the appropriate level of trust to support the consumer’s ability to evaluate the assertions and attestations made by the provider.</td></tr>
<tr><td><b>Step #</b></td><td><b>Activities</b></td></tr>
<tr><td>1</td><td>Consumer Management Agents decides that it wants to remove an asset</td></tr>
</table>

	from the Trusted Systems Domain. It request permission from the Trusted systems Domain Policy Store to remove the asset.
2	If the Consumer Management Agents removal request is granted then it request de-provisioning of the asset from the Provider Management Agent which removes the asset(s) from the Trusted Systems Domain and notifies the Consumer Management Agent of the retired assets. Assumption: This is what happens if the agreement between the consumer and the provider allows the incremental return of assets. We are assuming that the polices with regard to incremental return are consistent between the consumer and the provider. If incremental return is not allowed, all assets are returned.

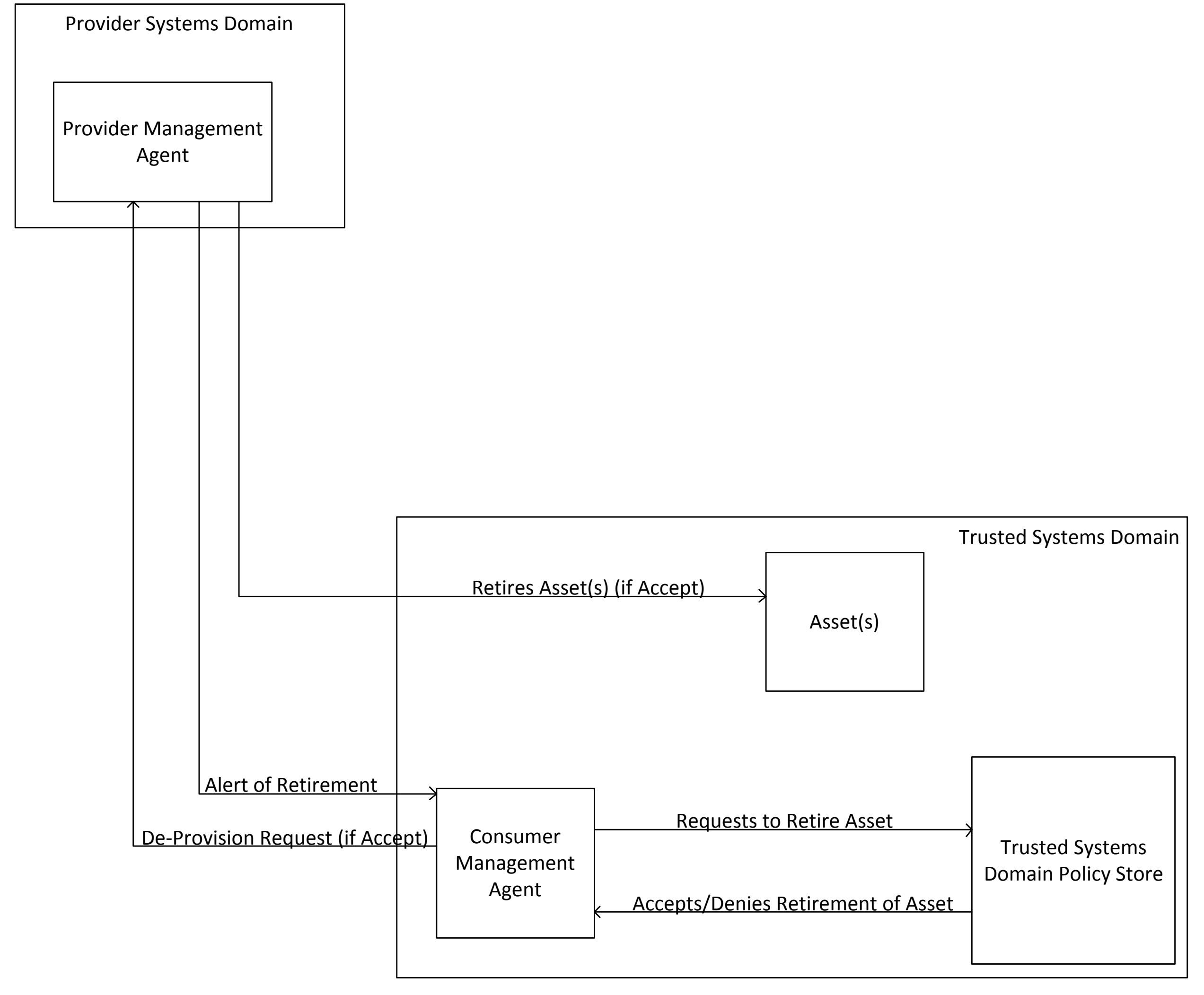
Issues / Key Requirements

- The use case assumes the following core functional use cases have been defined and are in use:
    - Establish a Trusted Systems Domain
    - Establish trust
    - Exchange Information in a trusted context
    - Assess and enforce policy statements
    - Provider policy allows for change to environment
    - Assess and enforce policy statements
- Need to provide scenarios that illustrate the types of policies that might be important in a TMI context

Contributors

Michael Donovan (HP), Mike Stolp (HP), Erik Visnyak (BAE Systems), Guerney Hunt (IBM)

Architectural Building Blocks


Provider Systems Domain
Provider Management Agent
Trusted Systems Domain
Retires Asset(s) (if Accept)
Asset(s)
Alert of Retirement
De-Provision Request (if Accept)
Consumer Management Agent
Requests to Retire Asset
Accepts/Denies Retirement of Asset
Trusted Systems Domain Policy Store

Threats

- The agents must be able to assess the degree of trust in the assertions made (agents could lie)
- Man in the middle attacks
- Replay attacks

Ref. #	**Use Case Name**
UC-6 Consumer	Operation of the surge capability within the Trusted System Domain

Description

This use case describes the steps required to operate a Trusted System Domain in a surge capacity where either by Consumer Policy initiation, Policy initiation or other mechanism a given Secure System Domain will be able to garner additional resources needed to continue a given level of service due to additional capacity requirements this use case will have an initial set of steps with additional scenarios attached but is written from the context of the provider.

Step #	Activities
1	The Consumer Management Agent detects a condition where additional resources are needed and queries to the Trusted Systems Domain Policy Store to see if the required resources are within policy. The Trusted Systems Domain Policy Store indicates whether the request is within policy
2	If the request for additional resources is within policy then the Consumer Management Agent forwards a request to the Provider Management Agent to provision additional assets within the Trusted Systems Domain.
3	If Provider Management Agent identifies available assets compliant with the Provider Domain Policy Store, .the Provider Management Agent provisions assets within the Trusted Systems Domain, transfers control of the assets to the Trusted Systems Domain, and alerts of Consumer Management Agent of the provisioned assets.
4	Consumer Management Agent validates and attests the provisioned assets against the Trusted Systems Domain Policy Store. If the assets are rejected for any reason control of the assets will be returned to the Provider Management Agent.

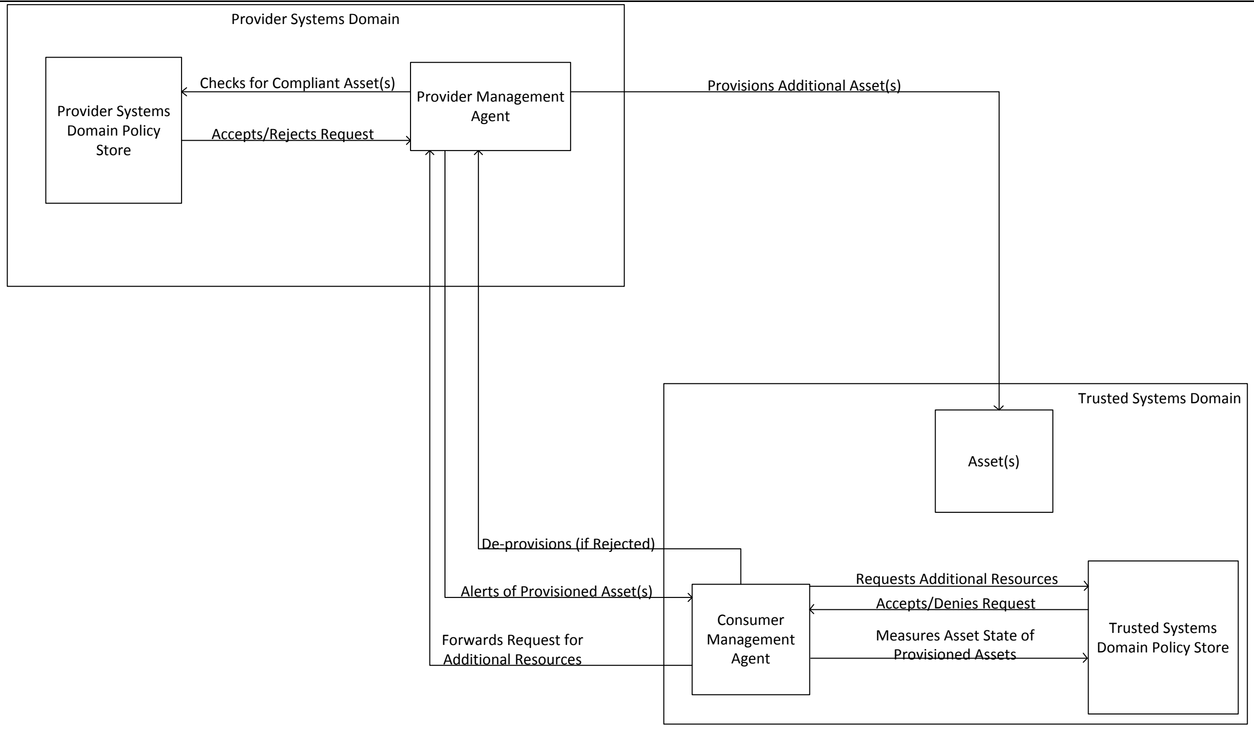
Issues / Key Requirements

- The use case assumes the following core functional use cases have been defined and are in use:
    - Establish a Trusted Systems Domain
    - Establish trust
    - Exchange Information in a trusted context
    - Assess and enforce policy statements
    - Provider policy allows for change to environment
    - Assess and enforce policy statements

Contributors

Michael Donovan (HP), Mike Stolp (HP), Erik Visnyak (BAE Systems), Guerney Hunt (IBM)

Architectural Building Blocks

 Provider Systems Domain Provider Systems Domain Policy Store Checks for Compliant Asset(s) Accepts/Rejects Request Provider Management Agent Provisions Additional Asset(s) Trusted Systems Domain Asset(s) De-provisions (if Rejected) Alerts of Provisioned Asset(s) Forwards Request for Additional Resources Consumer Management Agent Requests Additional Resources Accepts/Denies Request Measures Asset State of Provisioned Assets Trusted Systems Domain Policy Store
Threats
- The agents must be able to assess the degree of trust in the assertions made (agents could lie) - Man in the middle attacks - Replay attacks

Ref. #	**Use Case Name**
UC-7 Consumer	Audit of policy within the Trusted Systems Domain.
Description	
The main idea is to describe the ability to provide traceability of policy activities within the Trusted Systems Domain providing an audit capability to detect compliant and noncompliant activities. Note the Consumer Domain and Provider Environment may or may not be different organizations but must have some working relationship so the provisioning systems can establish the appropriate level of trust to support the consumer's ability to evaluate the assertions and attestations made by the provider.	

Step #	Activities
1	Consumer Management Agents make operational requests within the Trusted Systems Domain that are forwarded to the Consumer Audit Agent.
2	The Consumer Audit Agent evaluates the Consumer Management Agents operational request data from assets (based on policy) within the Trusted Systems Domain.
3	The Consumer Audit Agent alerts (based on policy) designated Consumer Management Agents of critical audit conformance and non-conformance events.

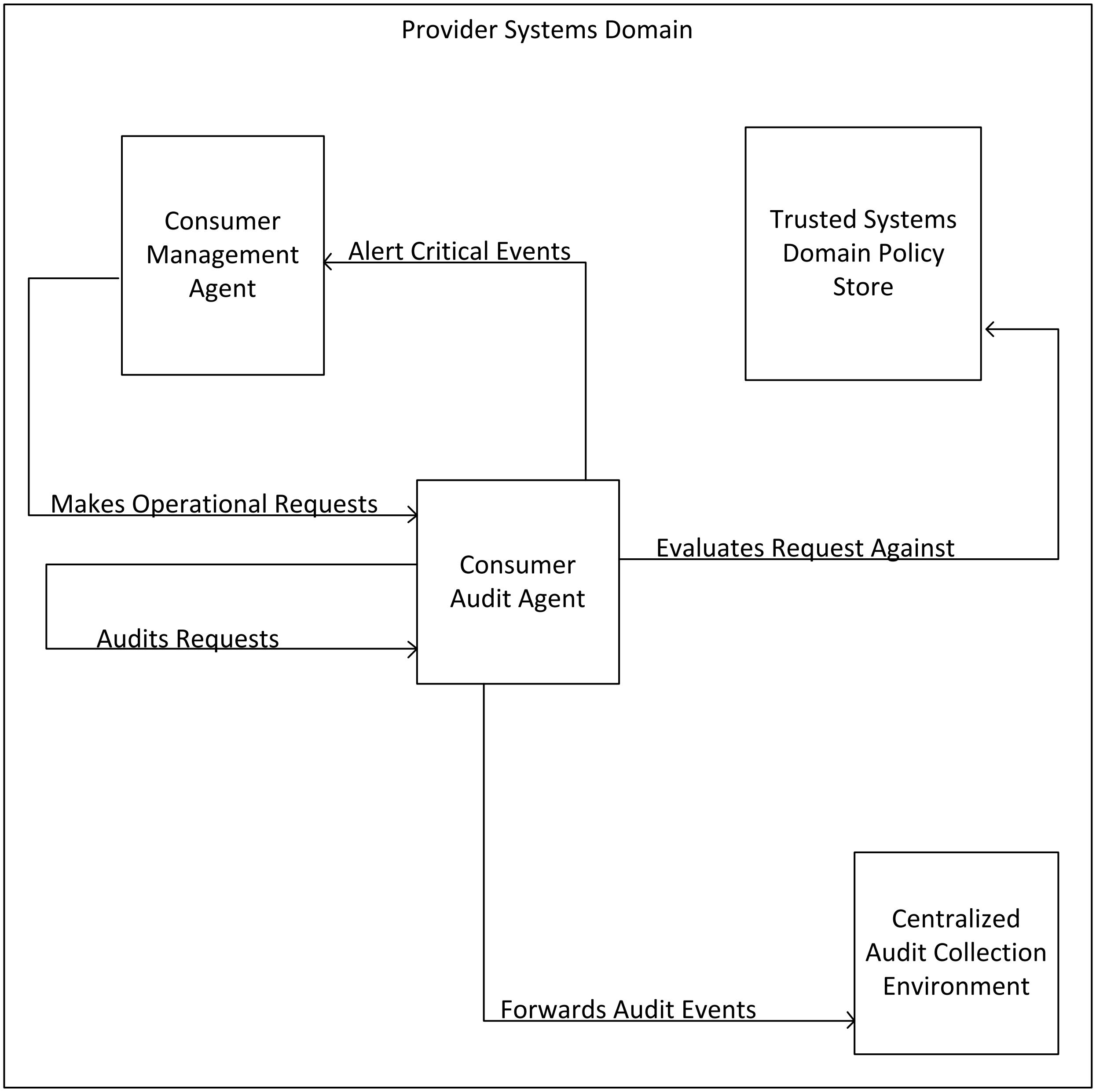
Issues / Key Requirements

- The use case assumes the following core functional use cases have been defined and are in use:
    - Establish a Trusted Systems Domain
    - Establish trust
    - Exchange Information in a trusted context
    - Assess and enforce policy statements
    - Provider policy allows for change to environment
    - Assess and enforce policy statements
- Need to provide scenarios that illustrate the types of policies that might be important in a TMI context

Contributors

Michael Donovan (HP), Mike Stolp (HP), Erik Visnyak (BAE Systems), Guerney Hunt (IBM)

Architectural Building Blocks


Provider Systems Domain
Consumer Management Agent
Alert Critical Events
Trusted Systems Domain Policy Store
Makes Operational Requests
Consumer Audit Agent
Evaluates Request Against
Audits Requests
Centralized Audit Collection Environment
Forwards Audit Events

Threats

- The agents must be able to assess the degree of trust in the assertions made (agents could lie)
- Man in the middle attacks
- Replay attacks

2.8 TMI Multi-Tenant Use Case Scenarios

In this section we will discuss the scenarios that detail actual situations that TMI issues are dealt with. At this time the focus is on creating and solidifying the Generic, Consumer and

Provider Use Cases that will form the frame work or basis of the TMI standard. This section will be filled out later

2.9 Uncategorized Use Cases

UC #	Description	Status