REFERENCE

Trusted Multi-Tenant Work Group

Trust Assessment Framework

Family "2.0"
Level 02 Revision 48
May 23, 2017
Final

Contact: admin@trustedcomputinggroup.org

TCG

TCG Published

Copyright © TCG 2003 - 2017

Disclaimers, Notices, and License Terms

THIS DOCUMENT 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, DOCUMENT OR SAMPLE.

Without limitation, TCG disclaims all liability, including liability for infringement of any proprietary rights, relating to use of information in this document and to the implementation of this document, 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 document 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 documents 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 document licensing through membership agreements.

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

Copyright ©2017 TCG

Acknowledgements

Michael Donovan, Hewlett Packard Enterprise

Mike Stolp, Hewlett Packard

Hagen Lauer, Huawei Technologies

Michael Eckel, Huawei Technologies

Yi Zhang, Huawei Technologies

Guerney Hunt, IBM

Dave Challener, John Hopkins University Applied Physics Lab

Christoph Ernst, Swisscom

Anne-Rose Gratadour, Thales Communications and Security

Chris Anderson, United States Government

Mike Boyle, United States Government

Andrew Tarbox, Wave Systems Corp.

Derek Tsang, WinMagic, Inc.

Ira McDonald, Consultant

Table of Contents

Copyright ©2017 TCG

1. Scope and Audience

As enterprises and individuals move into more complex hybrid environments with services spread across mobile apps, cloud service providers and distributed ecosystems it is imperative that we find a way to manage the trust relationships that make the distribution of responsibility work. This is more than just validation of the identity of an end user or even the state of a single device. Enterprises need a framework that supports assessment in a way that accounts for a dynamic environment whether an action should be taken or not. It is not enough to ask a binary question, “Do I trust this app?” Enterprises must be able to ask a much more nuanced series of questions, starting with “do I trust the ecosystem of participants in this action enough to take the action?”

This document is intended to fill the gap in the industry between the definitions of Risks and Trust. Risk is well defined but trust is not well defined. This document is also a complement to the ITU-T X.1254 “Entity authentication assurance framework” recommendation assurance levels for electronic identity to establish a definition of trust levels [1]. The intended audience of this document is those business and technical leaders who would be involved in or responsible for the decision to utilize a multi-tenant infrastructure or to move a current in house capability to a multi-tenant infrastructure. An example scenario of applying the concepts to a multi-tenant infrastructure is supplied in section 5, to help make the concepts concrete.

2. References

[1] ITU-T X.1254 (09/2012) Series X: Data networks, Open System Communications and Security; Entity Authentication Assurance Framework

[2] ISO Guide 73:2009 Risk Management Vocabulary

[3] IETF, Key words for use in RFCs to Indicate Requirement Levels, RFC 2119, March 1997

[4] Webster’s Ninth New College Dictionary: 1986 Merriam-Webster

[5] New Oxford American Dictionary, Second Edition; Oxford University Press, 2008; Kreuzfeldt Electronic Publishing GmbH, Hamburg (Germany)

[6] TCG Glossary of Technical Terms, http://www.trustedcomputinggroup.org/wp-content/uploads/TCG_Glossary_Board-Approved_12.13.2012.pdf

[7] Trusted Multi-Tenant Infrastructure Work Group Reference Framework, https://trustedcomputinggroup.org/trusted-multi-tenant-infrastructure-reference-framework/

[8] Trusted Multi-Tenant Infrastructure Work Group Use Cases, https://trustedcomputinggroup.org/tcg-trusted-multi-tenant-infrastructure-use-cases/

[9] IETF RFC 4949 Internet Security Glossary, Version 2, https://tools.ietf.org/html/rfc4949

Copyright ©2017 TCG

3. Terms

This section only defines terms that are unique to this specification. The TCG glossary of technical terms ([6]) and the IETF Internet Security Glossary ([9]) are the default definitions used within this document.

4. Trust Maturity Model

Trust is a key to relationships, digital or analog; consequently, an explicit or implicit “Trust Maturity Model” is essential to understanding the usage of a Trusted Multi-Tenant Infrastructure (TMI). Trust itself is not independent of other factors. Words such as risk and assurance are concepts that are implicitly or explicitly factored into trust. In the context of a multi-tenant infrastructure trust is a critical component. Trust is not a binary concept, but a relative one.

> **Trust**: Assured reliance on the character, ability, strength, or truth of someone or something [4]; firm belief in the reliability, truth, ability, or strength of someone or something [5].
>
> **Assurance**: Positive declaration intended to give confidence [5]

Trust in the context of trusted computing has a more complex definition defined by the TPM specifications, “Trust is the expectation that a device will behave in a particular manner for a specific purpose.” [6]. This is fine within the scope of an individual device. However within the scope of the TMI, the definition of trust has to address end-to-end-trust. For other situations, as the definition illustrates, trust is expressed in relation to something. The decision whether or not to trust something or someone is relative to other factors such as risk and the ability to mitigate the risk. Before the level of trust can be determined, what is at risk must be determined. If nothing is at risk, then the level of trust is immaterial and therefore it is easy to express trust. However, if there are catastrophic risks (or consequences) then there is a higher level of assurance needed to establish an appropriate level of trust.

Users of a multi-tenant infrastructure need to have a practical method to determine when such an infrastructure should be used. There are existing financial tools that help the user determine if there is a financial benefit for such a move. There are regulatory frameworks that guide a user on compliance for their industry. In some cases, there are laws that govern the placement of some types of information. This document exists to help the users understand what they need to evaluate to determine whether any gain they may perceive is proportional to the risk they are taking.

The TMI model has two primary components Impact and Assurance, each of which contains two subcomponents. Impact represents a combination of the likelihood of occurrence and the value at risk. Assurance represents the rights an owner has combined with the enforcement mechanism that protects the party’s rights.

The TMI Trust Assessment Framework includes in “**impact**” the likelihood of occurrence combined with an assessment of the **value** at risk. However, it is easy to see that these concepts are tightly coupled. If there is zero possibility that the event will occur, then there is no value at risk. Determining the likelihood of occurrence involves an evaluation of threats. The likelihood of occurrence is important, so it is defined as independent of value, and impact is computed as some function of the two.

The next factor that is associated with the understanding of trust is **assurance**. Much of the process of establishing and maintaining trust involves the exchange of statements about a set of facts, measurements, or observations. The degree to which a party is able to independently verify the statements affects the willingness of parties to rely on those statements. Related to assurance is the concept of **rights** granted to an entity to exert control over an asset. Restriction and enforcement of appropriate rights can decrease the assurance threshold. The second factor in assurance is

enforcement. Although enforcement is loosely associated with risks, the other way to think about this is; what is the likelihood of a violation of trust being discovered and what consequences (or penalties) will result? These are the basic issues that affect the establishment of trust.

4.1 Trust

Trust is more complex than having either no trust or complete trust.

For the TMI Trust Assessment Framework, the four levels of trust are defined as follows:

- Minimum Trust (Level 1) = Little or no confidence in the entity
- Moderate Trust (Level 2) = Some confidence in the entity
- Substantial Trust (Level 3) = High confidence in the entity
- High Trust (Level 4) = Very high confidence in the entity

The term "entity" can be replaced by any expressed attributes of a TMI or replaced by the owner and/or operator of a TMI. The attributes include identity, policy, enforcement, compliance, reputation, and prior experience. These levels of trust can be thought of as four points on a line segment with Low the endpoint on the left and Very High the endpoint on the right and the other points uniformly spaced resulting in a continuum between them.

4.1.1 Minimum Trust

Minimum trust in an attribute, owner, or operator of a TMI it means that there is insufficient evidence that the attribute (owner or operator) is trustworthy and consequently you are not willing to have anything of value, even minimum value, dependent upon the attribute (owner or operator).

4.1.2 Moderate Trust

Moderate trust in an attribute, owner, or operator of a TMI it means that there is evidence that the attribute (owner or operator) has limited trustworthiness. There are no known significant issues, but the data collected does not suggest that items of moderate or greater value should be dependent upon the attribute (owner or operator).

4.1.3 Substantial Trust

Substantial trust in an attribute, owner, or operator of a TMI means that the attribute (owner or operator) is trustworthy. There are no known significant issues. There are credible testimonies to the trustworthiness of the attribute (owner or operator). Violations of an agreement can be easily detected and there are functioning enforcement mechanisms. Consequently, items of substantial value can be dependent upon the attribute (owner or operator).

4.1.4 High Trust

High trust in an attribute, owner, or operator of a TMI means that the attribute as implemented contains all of the desired properties with sufficient detection and enforcement mechanisms. It also means that the operator (or owner) of the TMI and its operation meets or exceeds the highest standard of the organization that needs to extend trust. The data collected indicates that any information that depends on the attribute owner or operator is as protected with the same or greater diligence as the owning organization combined with sufficient detection and enforcement mechanisms. Consequently, almost all data can be dependent upon the attribute, owner, or operator.

4.2 Risk

Risk is a similarly complex subject. The ITU-T recommendation previously cited asserts that risks have three factors "the consequences of an authentication error and/or misuse of credentials, the resultant harm and impact, and their likelihood of occurrence."[1] Because the actual consequences vary with the situation in this model we only include the impact and the likelihood. In choosing these terms we require the user to identify the consequence and assign a likelihood and impact[2].

Risk has levels associated with trust, but is independent of trust. The lowest level is no risk and the highest level is catastrophic risks. The intermediate risk levels can be labeled the same as the intermediate levels of Trust. It would be unusual or unwise to take catastrophic risks with an entity with which you have no trust. However, it seems obvious that it is easy to take no risks with an entity with which you have complete trust.

4.2.1 Likelihood

Likelihood can also be categorized [2] into three levels:

- Low – Unlikely to occur. Possibly due to the difficulty of achievement or the cost to achieve vs. the benefit gained
- Moderate - Potential exists to realize the risk. The means, opportunity and motivation exist but may not be high enough to warrant the attempt
- High – Attempts to realize the risk are certain or near certain. The means, opportunity and motivation exist

An organization must assess the threat, know who may benefit, understand the potential for accidental realization and determine if mitigation policies can be established to offset the risk.

4.2.2 Impact

ITU-T X.1254 identified six categories of **harm**:

- Inconvenience, distress, or damage to standing or reputation
- Financial loss or liability
- Harm to programs or interests
- Unauthorized release of sensitive information
- Personal safety
- Civil or criminal violations.

This model accepts all six. This model also accepts the four **degrees of impact** defined by ITU-T X.1254. The level of importance of each harm has to be determined by the individual company. There is an implied order here, but each company **should** determine their own order of importance.

---

[1] For an example of how to apply this framework see section 5.

[2] Figure 1 in section 5.1 is an example table where all combinations have been evaluated.

- **Minimum—**at worst, limited, short-term inconvenience, distress or embarrassment to any party.
- **Moderate—**at worst, serious short term or limited long-term inconvenience, distress or damage to the standing or reputation of any party.
- **Substantial—**improper disclosure could result in a substantial risk for financial loss.
- **High—**severe or serious long-term inconvenience, distress or damage to the standing or reputation of any party.

It is important to note that the precise definition of these terms will depend on the role within the multi-tenant infrastructure. We use the term "any party" to refer to customer, user, provider, broker, and intermediary. If an organization is using a multi-tenant infrastructure it will evaluate the impact in terms of the effect on the organization. This includes the impact to its customers. When an infrastructure provider is evaluating impact, it is primarily concerned about the impact to its infrastructure and to its customers. It would also be concerned about the impact to customers of customers, etc. but that may depend on where it has insight into these consequences. It is also important to note that often time a harm can have multiple consequences. In such cases, determining the level of impact will involve a judgement call. There are two ways to classify the impact; place the harm in the category of its highest consequence or place it in the category of its root cause. This list is cumulative in the sense that higher impact may also have lower impact but not the other way around.

Applying these levels of impact to the six categories of harm yields the following definitions.

4.2.2.1 Inconvenience, distress, or damage to standing or reputation

The lowest type of impact is divided into categories as follows:

- **Minimum—**at worst, limited, short-term inconvenience, distress, damage or embarrassment to the standing or reputation of any party.
- **Moderate—**at worst, serious short term or limited long-term inconvenience, distress, or damage to the standing or reputation of any party.
- **Substantial—**substantial inconvenience, distress or damage to standing or reputation of any party.
- **High—**severe or serious long-term inconvenience, distress or damage to the standing or reputation of any party (ordinarily reserved for situations with particularly severe effects or which affect many individuals).

By inconvenience we mean something occurring that has no permanent after-effect, a one time, short lived event. Incorporated into this is the concept that there is an easy or straight forward work around. Distress and damage are governed by inconvenience. If the damage or distress were permanent or long-lasting, it does not fall into this category. We realize that short term and long term are relative terms. Of necessity, each institution has to determine the difference.

It is important to note that all of these are of limited scope. However, the length of the inconvenience varies with the degree minimum, moderate, substantial or high.

In general, this category does not cause significant financial loss.

4.2.2.2 Financial loss or liability

When harm gets to the point where it impacts the bottom line in a noticeable manner, it falls into this category. For a large organization, it will probably be necessary to set a specific minimal value which shifts an impact into this category. For smaller organizations a recommendation would be to use a specific percentage of a key financial measure.

- **Minimum—**at worst, an insignificant or inconsequential unrecoverable financial loss to any party, or at worst, an insignificant or inconsequential liability.
- **Moderate—**at worst, a serious unrecoverable financial loss or liability for any party.
- **Substantial—**substantial financial loss or substantial liability for any party.
- **High—**severe or catastrophic unrecoverable financial loss to any party; or severe or catastrophic liability.

The concept here is that a high or substantial degree of financial impact is likely to be reported on a quarterly or annual basis (for publicly traded companies). Moderate and minimum would be reportable to an appropriate authority in the organization. The basic concept here is that each organization needs to establish guidelines, value, to separate these categories. As before, a simple approach is to set the division points as percentages of a key financial measure or some computation on a set of financial metrics.

4.2.2.3 Harm to programs, interests, or reputation

This category describes long lasting harm or damage to ongoing programs, interests, relationships, or reputation. This can include financial harm. It is also possible for a harm to impact a program or interest without having significant financial impact. An example of this category is where some harm causes a loss of trust with a key partner and as a result the partner changes their relationship with the company. A second illustration is a harm that significantly affects the public interest of the company. Long lasting harm to reputation may change the terms on which partners will agree to contracts or influence public perception of the party to the point there is long lasting damage to the enterprise. Each of these instances can have significant financial impact. However, generally long lasting harm to a program or interest is farther reaching than the financial impact, consequently the harm should be assessed in this category. The degree of the harm is described as follows:

- **Minimum—**at worst, limited, short-term inconvenience, distress or embarrassment to a program or interest.
- **Moderate—**at worst, serious short term or limited long-term inconvenience, distress or damage to the standing or reputation of any program or interest.
- **Substantial—**substantial harm to the standing or reputation of any programs or interest.
- **High—**severe or serious long-term inconvenience, distress or damage to the standing or reputation of any program or interest (ordinarily reserved for situations with particularly severe effects).

4.2.2.4 Unauthorized Release of sensitive information

The unauthorized released of sensitive information can have a financial impact or impact a program or interest. It can also be independent of the other two harms. For example, if the unauthorized release of sensitive information is related to some past action that has no bearing on current programs it may not harm a program or interest or have any financial impact. A different example is the unauthorized release

of sensitive information related to a negotiation between two parties. It could be contract negotiations or acquisition negotiations. Either one could significantly harm a program or interest and have significant financial impact. The severity of the release is classified as follows:

- **Minimum—**at worst, a limited release of limited sensitive information that may cause a short-term inconvenience, distress or embarrassment to any party.
- **Moderate—**at worst, a release of sensitive information that can cause serious short term or limited long-term inconvenience, distress or damage to the standing or reputation of any party.
- **Substantial—**a substantial release of sensitive information exposing the organization or confidential information the organization holds.
- **High—**a substantial release of sensitive information that causes severe or serious long-term inconvenience, distress or damage to the standing or reputation of any party (ordinarily reserved for situations with particularly severe effects or which affect many individuals).

4.2.2.5 Personal Safety

Any harm that affects the personal safety of individuals or groups falls into this category. Obviously something that affects personal safety can also cause a civil or criminal violation as well as some of the previous harms. However, if the most direct cause is an exposure to personal safety which consequently causes other harms, it should fall into this category. The severity is classified as follows:

- **Minimum—**at worst, limited, short-term inconvenience, distress or embarrassment to any individual.
- **Moderate—**at worst, serious short term or limited long-term inconvenience, distress, injury (recoverable) or damage to the standing or reputation to one or more individuals.
- **Substantial—**a substantial impact to the personal safety of one or more individuals potentially resulting in serious injury, injury to reputation, or loss of resources.
- **High—**loss of life, severe or serious long-term injury, inconvenience, distress or damage to any individual.

4.2.2.6 Civil or Criminal Violation

Any harm that causes a civil or criminal violation fall into this category. The severity is classified as follows. If the harm immediately causes a civil or criminal violation, then it should fall into this category even when other harms are a result. The severity is classified as follows.

- **Minimum—**at worst, limited, short-term fine or restriction on any party.
- **Moderate—**at worst, a significant fine or long-term restriction for any party.
- **Substantial—**a significant fine with probation or incarceration for guilty parties.
- **High—**incarceration, severe or serious long-term or irrevocable restrictions, for individual or party (ordinarily reserved for situations with particularly severe effects).

4.3 Mitigation of Risks

4.3.1 Assurance

Assurance is related to the ability to verify assertions made by an entity. For hardware assets, a root of trust such as a TPM can protect the integrity of a measurement and potentially be used to certify that the measurement process has not been tampered with. One must be able to verify that the chain of evidence for the measurement is sound. For an operator or other party in a TMI, the ability to verify the authenticity, adherence to practices, adherence to policy, and reputation either through direct experience or from a trusted third party is important. The ability to verify compliance at random intervals and through differing mechanisms, such as remote inquiry or on-site inspection can influence the level of trust granted.

Obviously not all assurance comes from discrete measurements. Reputation, which can be gathered from a number of sources, is effectively part of assurance. Reputation cannot eliminate the need for some form of discrete measurement, but it may change the type and frequency of measurement. Reputation is affected by assurance received from trusted third parties.

4.3.2 Policy

The TMI Trust Assessment Framework assumes that policy is a set of testable statements describing a set of specific criteria necessary to mitigate the risks associated with using the TMI patterns to establish trust. The Trusted Multi-tenant Infrastructure (TMI) Work Group Reference Framework describes the use of policy within a multi-tenant infrastructure. Policy is used as tool to mitigate risks. Policy must be enforceable. The TMI Reference Framework ([7]), in section 3.1.3, describes how to determine, validate, and enforce policies. In section 3.4.2, it discusses how to provision, validate and enforce policies. At all times in this document and the reference framework policies are defined/assumed to be measurable and verifiable. Policy is central to the operation of a TMI and is discussed throughout the Reference Framework.

The consumer of a multi-tenant infrastructure cannot assume that all of the information needed to enforce policy is available or all of the actions required by policy are possible. The consumer must verify that the provider policy is consistent with their needs. Finally, the consumer must verify that the infrastructure has effective monitoring and enforcement mechanisms. Whether the provider represents IT services within the same organization or services provided to a large community the requirements and policies of the user/consumer should be defined and reconciled with the policies of the provider.

Each party, provider and consumer, should be able to clearly define, measure, monitor and enforce compliance with their policies. There may be more than 2 parties involved in managing policy compliance. There may be multiple providers with resources allocated in support of a consumer’s trusted systems domain.

4.3.3 Enforcement

For enforcement to be possible violations must be detectable. For violations to be detectable the policies governing the TMI must be measurable. If policies do not describe measurable events, operation, or outcomes, then violations cannot be detected and enforcement is impossible. The user of a TMI must

Copyright ©2017 TCG

verify that their policies governing use are measurable and that sufficient information is always available to measure the infrastructures adherence to its own policies.

The next obvious question is who or what enforces a violation of trust/Policy? What consequences exist for violating trust? There are four possible enforcement levels; no enforcement, enforcement by contract (civil agreement), enforcement by law (criminal), and enforcement by an irreversible mechanism. Not all levels may exist in every situation. An irreversible method is one where the consequences of enforcement cannot be reversed. For a TMI, the level of enforcement required should be a matter of policy. The consequences should be negotiated as part of the contract for use of the TMI. As previously mentioned, all policies must be measurable and actionable.

4.3.3.1 Rights

Whatever rights a user of a TMI has are established as a matter of policy and consequently must be measurable. Once a right is granted, it enables the enforcement of policy. Policy is used to provide assurance that the right is used as expected and enforcement to prevent improper use of the right. Just as organizations can be hierarchical, so can policy. The rights granted must be consistent throughout the hierarchy.

The consumer of a multi-tenant infrastructure intends to utilize the assets for a specific purpose. There are basically four fundamental rights that can be granted to an asset:

Access: The right to "access" the asset but no other right. Think of read only for a file. The user has the minimum possible capability.

Modify: In order to have modification rights, access rights are usually required. This is similar to write permissions for a file. No authority is granted to determine anyone else's rights to the asset.

Manage: The ability to monitor, control/configure and provision/de-provision independent from the other types of functional capabilities. The manager may or may not have access and modification rights to all aspects of the asset.

Full Control: The ability to grant and revoke access, any of the four rights, to other parties. If one has full control every aspect of the asset is under their control.

The exact number of levels of control is dependent on the asset. For example, some assets cannot be shared, consequently, there may be only full control or in some cases no manage level. Rights to resources must be aligned with the principle of least privilege. When applied to a TMI, least privilege says that the rights granted to each user (or component) must be the minimum required to accomplish their purpose (or legitimate purpose).

5. Applying the Assessment Framework

Within the patterns defined in the TMI Reference Model the user is called a consumer and the infrastructure provider is called the provider. Within the structure of the TMI it is incumbent upon the consumer and provider to populate the trusted identity store (TIS) with verifiable information about each of the parties and/or assets managed within the TMI. Each party must take ownership, in terms of responsibility for the accuracy of the supplied data. The data in the TIS must have integrity protection, meaning that all changes are detectable. Each data item in the TIS must only be changeable by the owner (authorized party associated with the consumer or provider). Access control on the items must be specified at the time of creation. The consumer and provider can use the data in the TIS to assist in the establishment of trust. Both parties must confirm that policies are in place to protect the assets.

The consumer of the TMI must know the value of the assets/IP/information they wish to place in the multi-tenant infrastructure. Concurrently the provider knows the value of assets they are willing to provide. The user needs to assess the risks of acquiring assets through the TMI. Similarly, the provider needs to assess the risk of providing an asset to the TMI. Both have to assess the risks of (or level or trust required) to work with the other party. The risk assumed is influenced by the assurance and enforcement mechanisms for violating trust. In general, a stronger enforcement mechanism will lead to lower risk. This does not mean that the highest level of enforcement implies the lowest level of risks because there are of other factors that affect risks.

This assessment framework is associated with the trust between two parties. The parties involved have to independently determine what is required for them to increase their level of trust in the other party. The parties must define:

What assets are being granted to or received from the other party?

The value of the assets, information, or intellectual property that the other party may have access to.

What tasks is required of the other party?

What kind of access rights are required to perform the task?

What kind of enforcement does each party require for a violation of trust?

What assurance mechanisms are in place to verify compliance?

What amount of trust does each party require for each level of risks?

What level of trust is required to grant the necessary rights to the other party?

5.1 Application

The TMI Trust Assessment Framework is applied either manually or automatically. Automatic application is accomplished though the policies expressed by the users and providers of the TMI. The framework indicates how those policies are utilized and how the TMI responds to policy violation. The manual side of use has multiple components.

- An assessment of the provider through non automatic means, e.g. Dunn and Bradstreet, web search, references, etc.
- An assessment of the value of the information/IP that will be exposed through the use of the TMI. This type of assessment would be guided by the internal polices of the entity exploiting a TMI. It would include building tables that would identify for each level of harm what type of trust would be

Copyright ©2017 TCG

considered sufficient to mitigate the potential impact (high, medium, low). The more comprehensive, the more accurate the risk exposure. It may be possible to automate some parts of this process.

- Implementation of enforcement mechanisms within the organization for those areas of extreme risk.
- Evaluation of the enforcement mechanisms of the TMI provider.
- Evaluation of external enforcement mechanisms.
- Explicit decision to utilize or not utilize a provider and an explicit decision as to what type of uses are permissible.
- Codification of these decisions into policies that can be enforced by the TMI management agents for the infrastructure. If the infrastructure has the capability to implement the design patterns defined in the TMI reference model then the enforcement can largely be automated. Otherwise the enforcement will be by corporate policy.

The table below shows an example mapping of the categories of harm with corresponding potential impact to suggest levels of trust required to mitigate the exposure. It is an example of the types of tables that the user of a TMI will have to either construct or accept. The levels of trust required for the same type of transaction with similar risks and potential impacts may vary by organization's business and risk tolerance policies. The two primary risk factors are impact and likelihood. Impact is a measure of the effect of violation upon the organization. Likelihood is a measure of the probability of occurrence. For each of the previously defined impacts[3], the likelihood varies from low to high. On the vertical axis we show the level of harm to the organization. The content of the table indicates the level of trust required to accept the potential impact of the associated harm.

Once the table is established, the consumer must confirm that the policies are in place to assure that the TMI operates with functional mitigations (assurance and enforcement) for all risks identified as acceptable. The consumer must also assure the mitigations are in place to prevent unacceptable risks. Development of this chart is key to the use of a TMI. Each consumer of a TMI must create and verify a table similar to the one below.

[3] Defined in section 4.2.2.

Level of Harm	Potential Impact											
	Minimum			Moderate			Substantial			High		
	Likelihood			Likelihood			Likelihood			Likelihood		
	Low	Med	High	Low	Med	High	Low	Med	High	Low	Med	High
1 Inconvenience	**T1**	**T2**	**T2**	**T2**	**T3**	**T3**	**T3**	**T3**	**T3**	**T3**	**T3**	**T3**
2 Financial Loss	**T2**	**T2**	**T3**	**T3**	**T3**	**T3**	**T4**	**T4**	**T4**	**T4**	**T4**	**T4**
3 Reputation/ Image	**T1**	**T1**	**T2**	**T2**	**T2**	**T3**	**T3**	**T4**	**T4**	**T3**	**T4**	**T4**
4 Unauthorized Release	**T1**	**T2**	**T2**	**T2**	**T2**	**T3**	**T3**	**T4**	**T4**	**T3**	**T4**	**T4**
5 Personal Safety	**T3**	**T3**	**T3**	**T3**	**T3**	**T3**	**T4**	**T4**	**T4**	**T4**	**T4**	**T4**
6 Civil Criminal	**T2**	**T3**	**T3**	**T3**	**T3**	**T4**	**T4**	**T4**	**T4**	**T4**	**T4**	**T4**

T1 = Minimum Trust
T2 = Moderate Trust
T3 = Substantial Trust
T4 = High Trust

Figure 1 Table indicating trust required based on the potential harm compared to the potential impact including likelihood of occurrence.

5.2 Example Scenario

The implementation scenario presented is part of a library of scenarios that will grow over time. Each scenario is selected to demonstrate the challenges to maintaining trust and accountability when implementing multi-tenant, multi-supplier infrastructure solutions.

5.2.1 Business Scenario - Mobility

The scenario presented here, and illustrated in Figure 1 represents the challenge of maintaining a reasonable level of performance and security when faced with the need to provide access to various assets for a mobile user. In some situations, the user moves further from the normal "home" of the corporate assets (or information). Consequently, to facilitate a reasonable experience it is necessary to move the asset (or information) closer to the location of the user. The movement of the user and the automatic movement of information potentially impacts the user's perceived performance or user experience. In other cases, the capacity limits of communication channels between the user and the asset (or information they need) make necessary interactions impractical or impossible.

One common scenario is that of a mobile business user who needs access to enterprise data as they move between home, office and remote (possibly customer) locations, often across a wide geographic

span. A wide degree of variability is introduced as the user connects back to the data across a corporate LAN or wireless network vs. a variety of local or remote mobile wireless network providers (possibly via a VPN). Users have a reasonable expectation that access to the information they need can be provided in a timely manner, as they will often abandon an access attempt after a relatively short time. It is also important to recognize and provide protection for corporate data based upon the criticality of the information, which may vary on a document by document basis. This balance of adequate security vs. performance is examined in this scenario.

5.2.2 Context

The scenario involves a business user with a need to access a corporate information store. The store contains information with multiple levels of risk to the enterprise were it to be compromised. This scenario assumes that the enterprise has appropriate access controls on sensitive information and that the infrastructure through which the user accesses the information is aware of the user's credentials, the type of device being utilized, and the user's location. The user accesses the information using a mobile device when not in the office. The enterprise has established a set of SLAs for user access performance that must be met. The enterprise also has policies that place restrictions on certain data that may not be moved outside of the enterprise and the corporate intranet. Information not so restricted could be hosted and accessed on approved devices external to the corporate intranet.

5.2.2.1 Execution Sequence

The details of the scenario are as follows:

1. A trust domain is established which consists of an information store, a communications channel and a mobile end-user device,
2. There is a consumer policy that describes a certain minimum acceptable performance characteristic for retrieving information
3. The user of the mobile device boards a plane and eventually reconnected to the communication channel at a remote location after landing
4. The user accesses the information store and the system detects that the performance policy can no longer be met
5. The consumer management agent identifies a provider in a location that will allow the performance requirements to be met and triggers migration of the information from the internal store to the new provider
6. The original provider was internal and the new provider is external, consequently the level of trust for the new provider must be established. The new level of trust and the location of the provider establish which information can be accessed (migrated) due to information protection policies
7. Once the change is made, monitoring continues, now in a multi-supplier, multi-tenant environment.

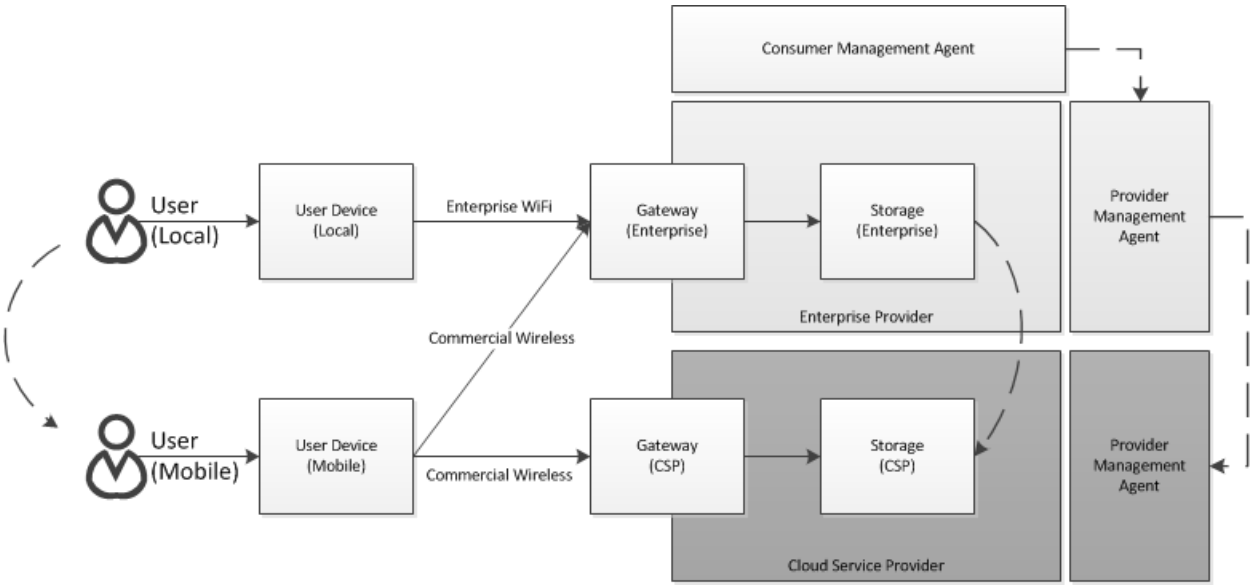

Figure 2, Scenario

5.2.2.1.1 Assessment

For the purposes of this example, we are assuming that the store contains information with multiple levels of risk to the enterprise were it to be compromised. The assumptions we are making for the scenario are:

1. User is going to access data that has a risk profile of:
    a. Inconvenience: Impact Minimal, Likelihood Moderate (T3 trust required)
    b. Financial: Impact Minimal, Likelihood Low (T2)
    c. Reputation: Impact Moderate, Likelihood Low (T2)
    d. Release of sensitive info: Impact Moderate, Likelihood Moderate (T2)
    e. Personal safety: Impact Minimal, Likelihood Low (T3)
    f. Criminal liability: Impact Minimal, Likelihood Low (T2)
2. The user accesses the information using a mobile device when not in the office.
3. The enterprise has established a set of SLAs for user access performance that must be met.
    a. Data to be accessed must be available in < 3 seconds
4. The enterprise also has policies that place restrictions on certain data that may not be moved outside of the enterprise and the corporate intranet.
    a. Moderate or above for sensitive info cannot be hosted outside the corporate network unless it remains in country
    b. No more than 4MB of sensitive data at a time can be migrated to an external store (user cache)
    c. Information with less restrictions could be hosted temporarily and accessed on approved devices external to the corporate intranet.

Trust Requirement: Using the trust assessment table illustrated in Figure 1, based on the information risk and likelihood profile of the data the mobile user will access we find that an overall trust level of T3 must be met. (ceiling (T3, T2, T2, T2, T3, T2) = T3)

Next, we need to look at the entities for which trust needs to be established, and the level of trust assigned to each:

Entity	Provider	Policy Modifier	Trust Level

Copyright ©2017 TCG

User			T4
User Device	Local		T3
	Mobile		T2
		Container or VDI	T2
		Trusted Device	T3
		Controlled White List	T4
Network	Corporate		T4
	Public		T1
		Encrypted E2E	T3
Gateway	Corporate		T4
	Public		T2
		Encrypted data	T3
Storage Service	Corporate		T4
	Public		T1
		Strong access controls	T2
		Encrypted at rest	T3
Replication Service			T3
Consumer Agent			T4
Provider Agent	Corporate		T4
	Public		T3
Cloud Provider	Public		T2
		Virtual Private container	T3

Figure 3, Entity and mitigation assessment

Now we can walk through the actions implied by the scenario. We apply the appropriate policy modifiers to the scenario segment to achieve the ability to perform the task.

5.2.2.1.2 Enterprise Access

As we look at the entities involved in the first part of the scenario, we can determine that no additive risk mitigations are necessary as the trust level meets or exceeds the minimum required for access to the information:

Entity	Trust Level
User Device, Local	T4
Network, Corporate	T4
Gateway, Corporate	T4

Storage Service, Corporate	T4
Consumer Agent	T4
Provider Agent, Corporate	T4

565

566 The overall Trust level is assessed to be T4 (floor (T4, T4, T4, T4, T4, T4) = T4)

567 As Trust Level 4 exceeds the assessed minimum trust level for the access path and transaction (T4 >
568 T3) then the agents allow the transaction to proceed without further action.

569 ***5.2.2.1.3 Mobile Access***

570 As we look at the entities involved in the second part of the scenario, we can determine that the minimum
571 trust level is not met and that policy mitigation and enforcement actions will need to be taken in order
572 for the access to occur.

Entity	Trust Level
User Device, Mobile	T2
Network, Public	T1
Gateway, Public	T2
Storage Service, Public	T1
Replication Service	T3
Consumer Agent	T4
Provider Agent, Public	T3
Cloud Provider, Public	T2

573

574 Overall Trust level is assessed to be T1 (floor (T2, T1, T2, T1, T3, T4, T3, T2) = T1)

575 As Trust Level 1 does not meet the minimum assessed trust level to provide an acceptable risk profile
576 the trust levels of the entities in the trust domain need to be mitigated to raise the end to end assessment
577 or the transaction cannot be performed.

578 Let’s look at each of the entities and policies that might be used to raise the level of trust:

579 User Device, Mobile: As we look at the table for policies that can impact the trust level, it appears the
580 use of a trusted mobile device will raise the level to T3 and ensuring that only certified apps are loaded
581 will raise to a T4. The use of a trusted device is enough to address this risk.

582 Network, Public: The use of end to end encryption (Encrypted E2E) of an acceptable type and strength
583 can raise the level of trust to the minimum required, T3. It is imperative to ensure that at no time is the
584 traffic in the clear over the public network. If this can be enforced, then the minimum trust level can be
585 achieved.

586 Gateway, Public: The use of end to end encryption of an acceptable type and strength can raise the
587 level of trust to the minimum required, T3. It is imperative to ensure that at no time is the traffic in the
588 clear over the public network. If this can be enforced, then the minimum trust level can be achieved.

Storage Service, Public: The use of public storage can be especially risky. While access controls alone only achieve a T2, their use in addition to encryption is good practice so the combination of both is recommended in this case and will raise the trust level to the minimum T3.

Cloud Provider, Public: The use of a virtual, private container and host in a public cloud can limit access from other cloud users and is sufficient mitigation with a trusted provider to raise the trust level to a minimum of T3.

5.2.3 Example Assessment Summary

So let's look at the reassessment of the trust level for the mobile transaction:

Entity	Inherent Trust + Mitigation	Resultant Level of Trust
User Device, Mobile	T2 + trusted device	T3
Network, Public	T1 + encryption	T3
Gateway, Public	T2 + encryption	T3
Storage Service, Public	T1 + encryption	T3
Replication Service	T3	T3
Consumer Agent	T4	T4
Provider Agent, Public	T3	T3
Cloud Provider, Public	T2 + virtual private	T3

Overall Trust level is assessed to be T3 (floor (T3, T3, T3, T3, T3, T4, T3, T3) = T3)

With the mitigation policies applied and enforcement monitoring in place through the trusted consumer and provider management agents, the transaction can proceed. The movement of data to a remote cache provided through a public cloud provider allows the performance and security policy requirements to be met.

6. Conclusion

What has been proposed in this framework is a way to extend the work of the Trusted Multi-tenant Infrastructure (TMI) working group to assess, in context, the elements of a transaction. Enabling enterprises to determine the risk and through policy decisions to determine the proper level of trust, assurance actions may be taken to maintain the level of trust in order to mitigate the inherent risks. It addresses the assertion that trust is not a binary state, but is variable in relation to whether sufficient trust exists to perform an action.

Using the assessment framework described, a participant in a transaction is able to:

1. **Define acceptable trust levels:** Develop a table that defines the level of trust necessary for the organization to reach an acceptable level of trust to perform an action.
2. **Perform risk assessment:** Assess the level of risk and the likelihood of risk occurrence against multiple type of threat.
3. **Determine minimum level of trust:** Apply the trust table against the risk assessment to determine the minimum level of trust required to perform the action.
4. **Assess transaction entities:** Assess each of the entities participating in an action to determine the inherent level of trust an organization places in the entity and potential policies that may be used to raise the level of trust.
5. **Manage the level of trust:** If an acceptable level of trust does not exist, use policy based mitigation that raises the level of assurance and enforcement capability to the point where the minimum level of trust exists. If an acceptable level of trust cannot be established, then an enterprise needs to determine the appropriate response; cancel the transaction or accept the risk.
6. **Perform the action within a trusted context:** Leverage the patterns from the TMI Reference framework to execute the action within the policy constraints defined once a trusted execution context has been established and can be monitored and managed.

While this may seem to impose a high level of overhead on a multi-tenant, multi-provider ecosystem, it is important to recognize that not all transactions will require the strict trust management overlay described here. Most day to day transactions are likely to take place within a context where a minimum level of trust already exists and the trust management effort is in monitoring the state of the trust environment for changes that might impact the level of inherent trust. There are, however, certain types of transactions that require special handling based on the criticality of the action or the sensitivity of the information. For these transaction types, this framework may be used at a more discrete level.

Between the openness of the Trust Assessment Framework and the TMI Reference Model, an organization is not bound to a specific hard architecture in order to manage a trusted platform environment. The reference model patterns may be applied to the types of entities that are found in the real world in combinations that the authors could not imagine or predict. The intent of this work is to provide a tool kit that allows for a repeatable approach to solving these end-to-end real world trust challenges.