Elements of a Trust Framework

A Conceptual Meta-Model

By Jeff Stollman
stollman.j@gmail.com

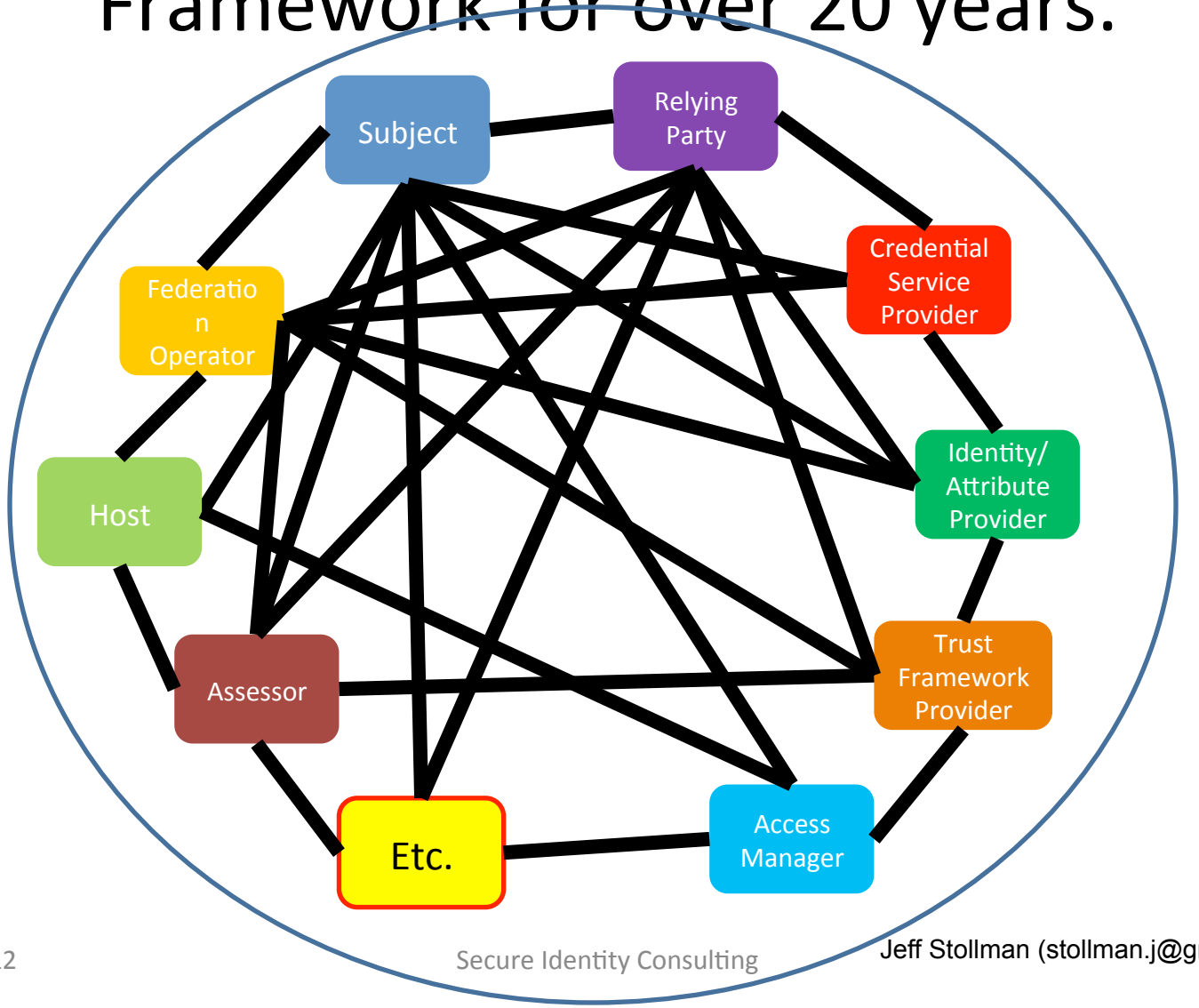
26 APRIL 2012

Agenda

- The Goal
- Why the goal has eluded us
- Solving the problem with certainty
  - Step 2: Problem Definition
  - Step 3A: Requirements Definition
  - Step 3B: Problem Modeling
    - 1. Trust Element Model
    - 2. Enumerating the Trust Elements

THE GOAL

We have been trying – without success – to create a General-Purpose Trust Framework for over 20 years.



What is a General-Purpose Trust Framework (GPTF)?

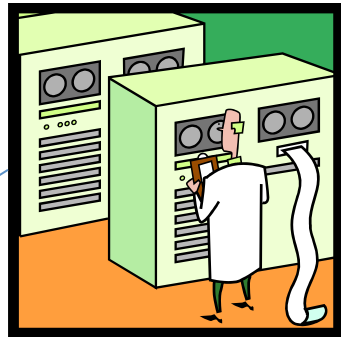
- The GPTF is an infrastructure that supports a wide array of interactions by extending trust to parties remote and/or unknown to us.
- This extension of trust facilitates these interactions by reducing the perceived risk of such interactions.

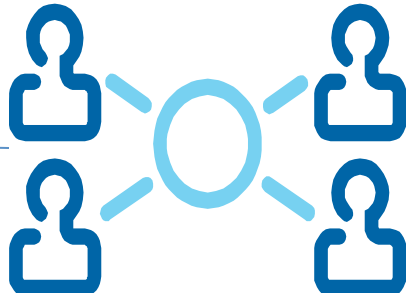
Characteristics of a GPTF

1. A GPTF is an infrastructure that supports a wide array of interactions, for a wide array of entities, over an array of assurance levels .
2. It operates by extending trust to parties remote and/or unknown to each other.
3. This extension of trust facilitates interactions by mitigating the perceived risks of such interactions.
4. The infrastructure consists of tools and processes, including laws, regulations, contracts and the legal infrastructure to enforce them.
5. It is global.
6. The GPTF is "general-purpose" because it supports a diverse array of interactions.

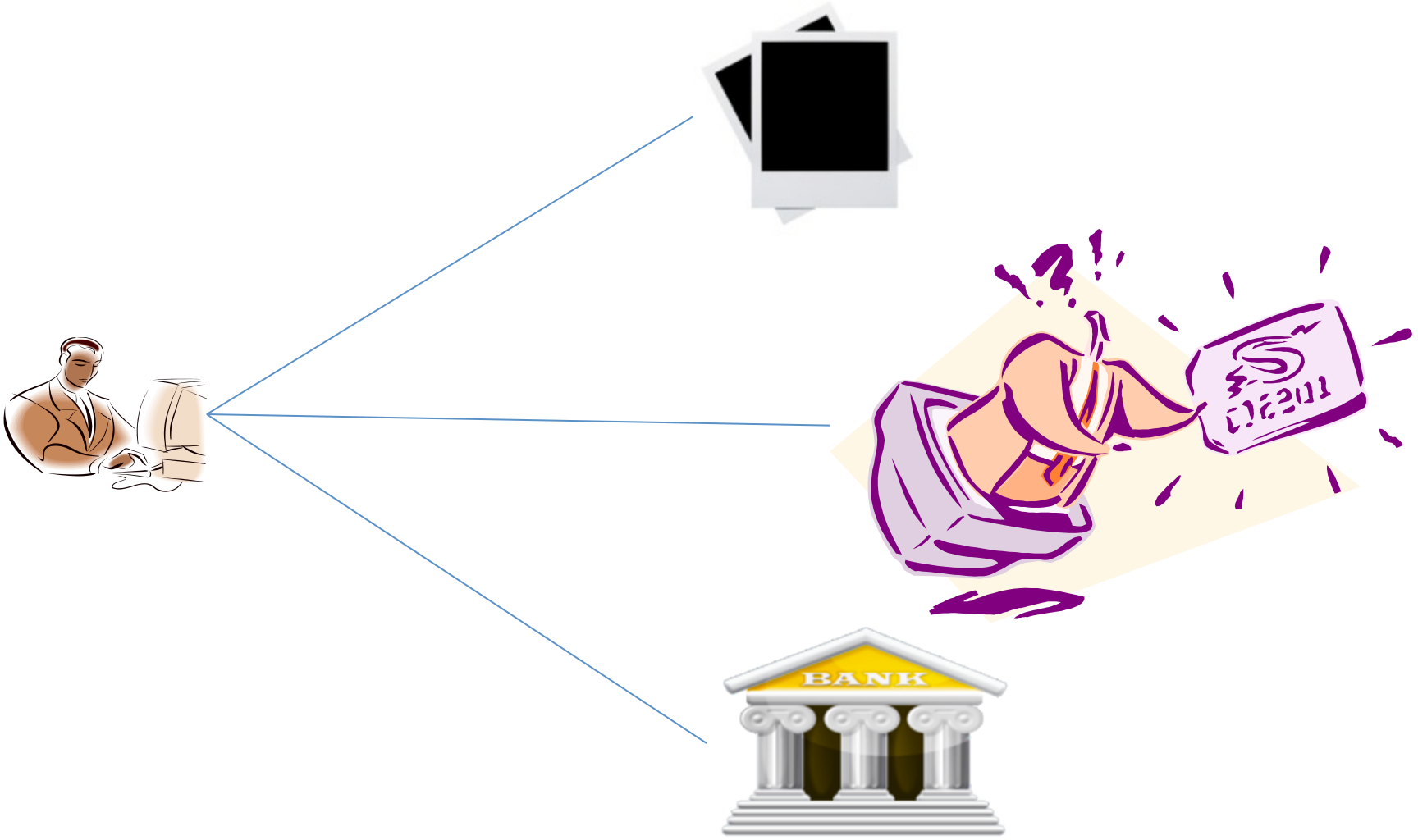
WHY THE GOAL HAS ELUDED US

The Birth of Identity

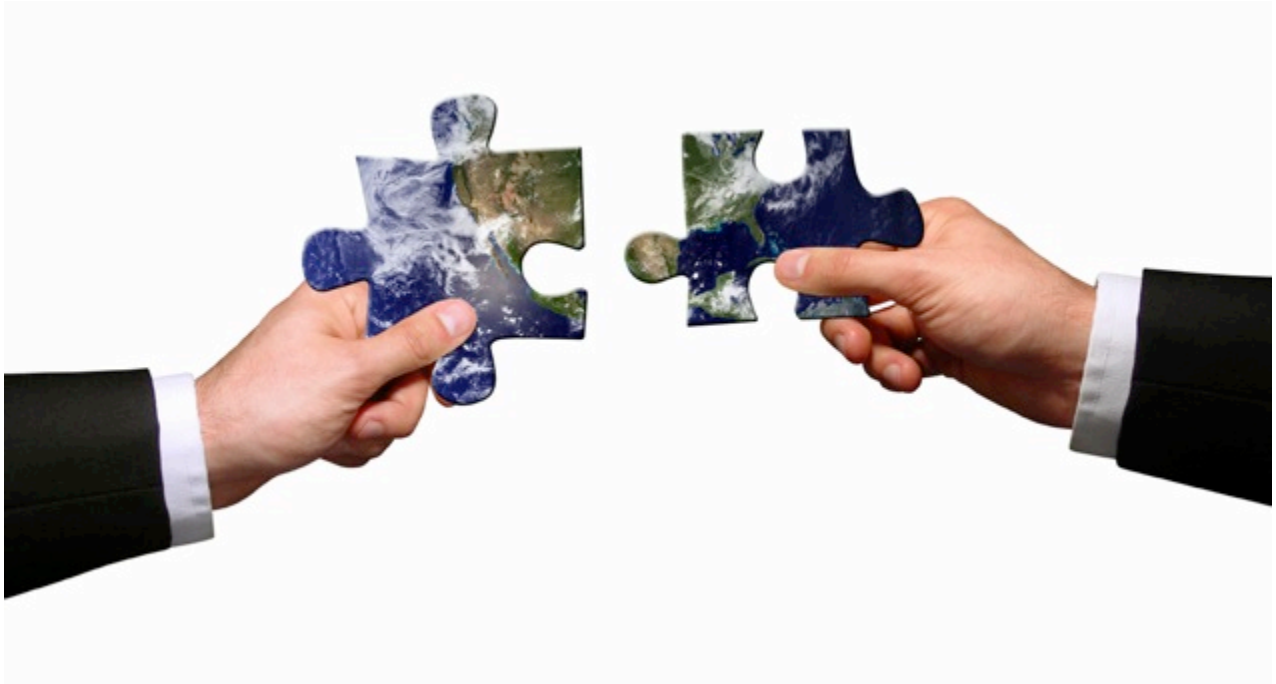




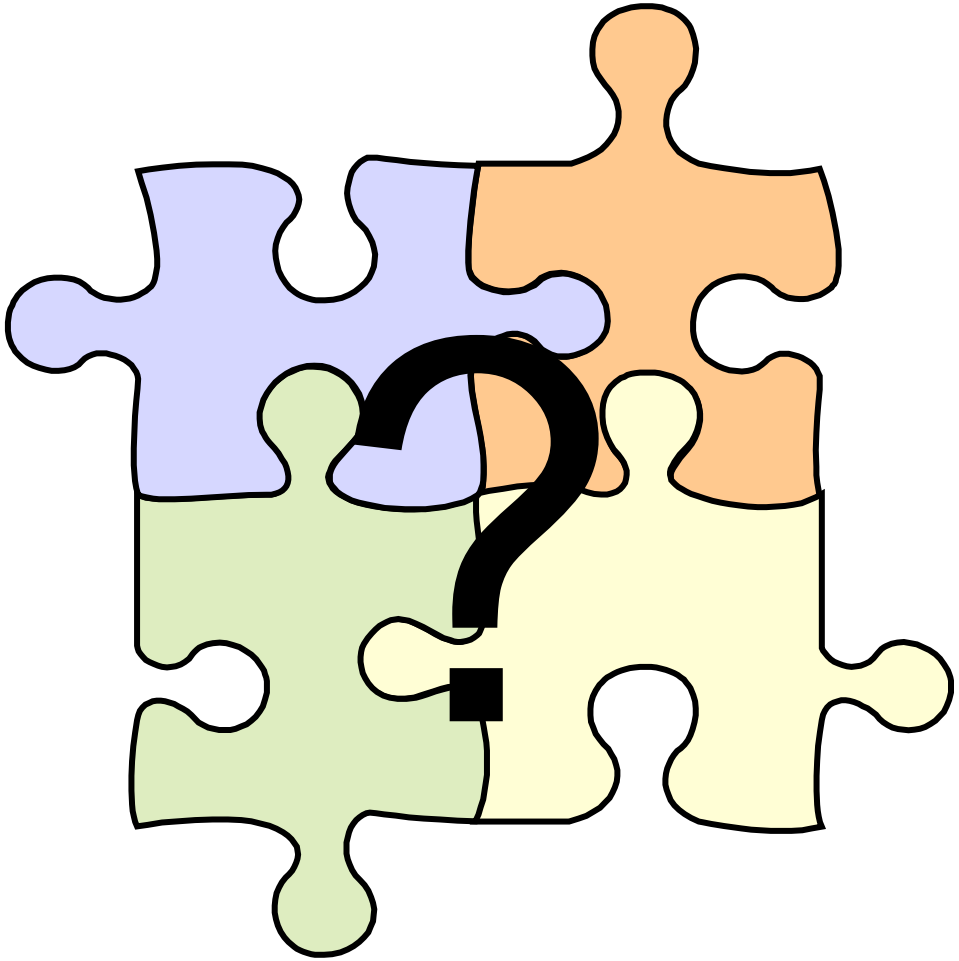
Extending the Identity Model



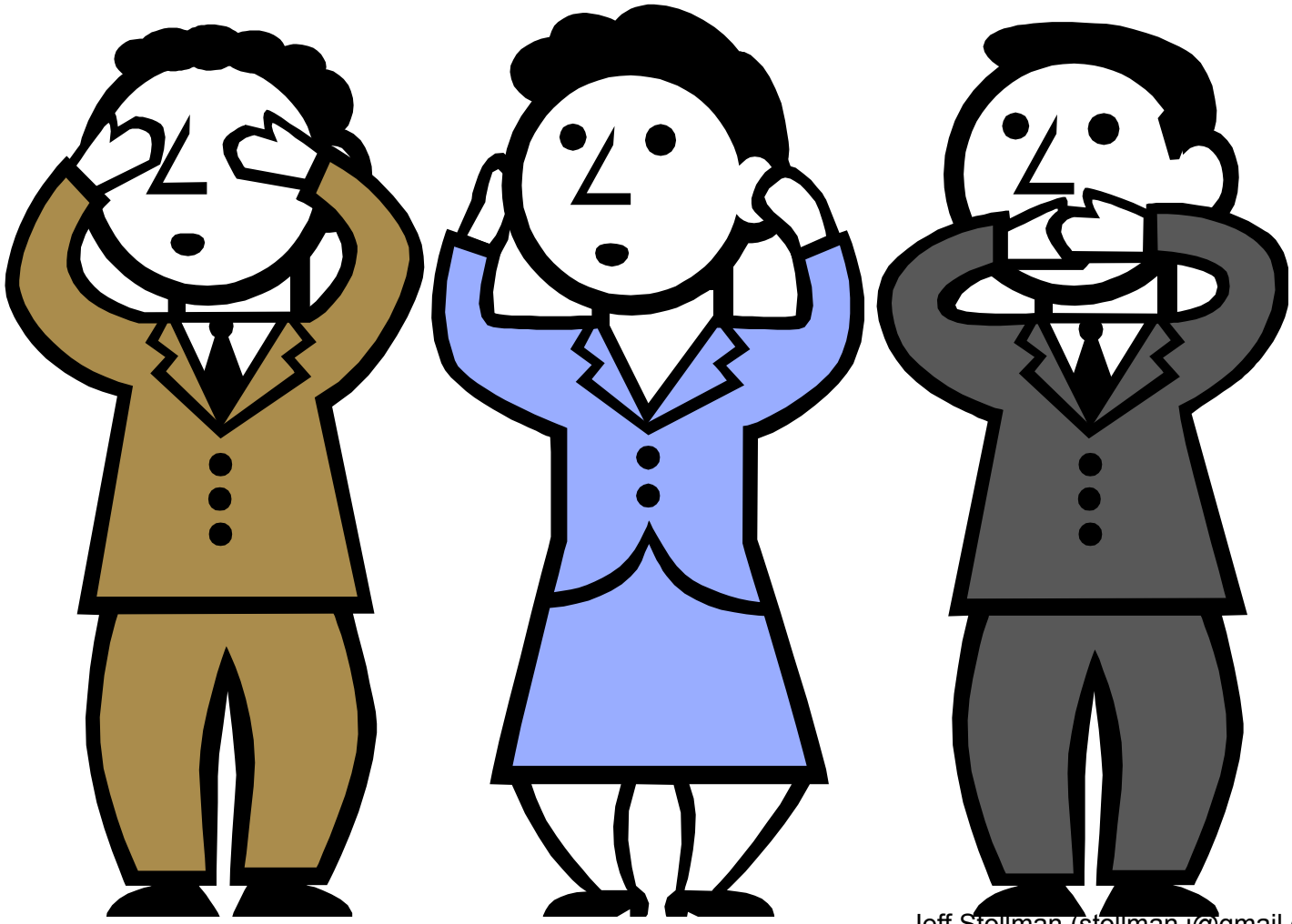
Thinking Big



Why not?



See no evil…

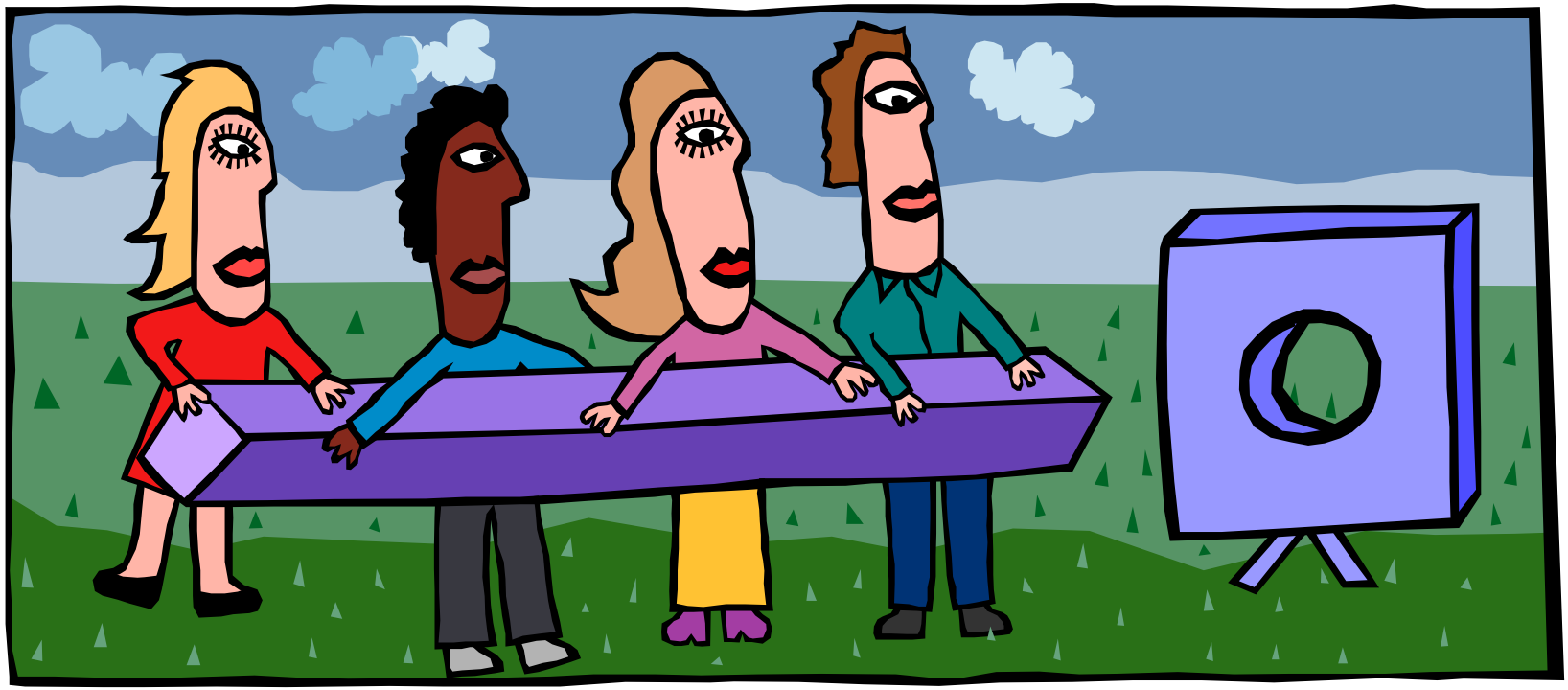


Solid foundation

Exercise

Are you a gambler?

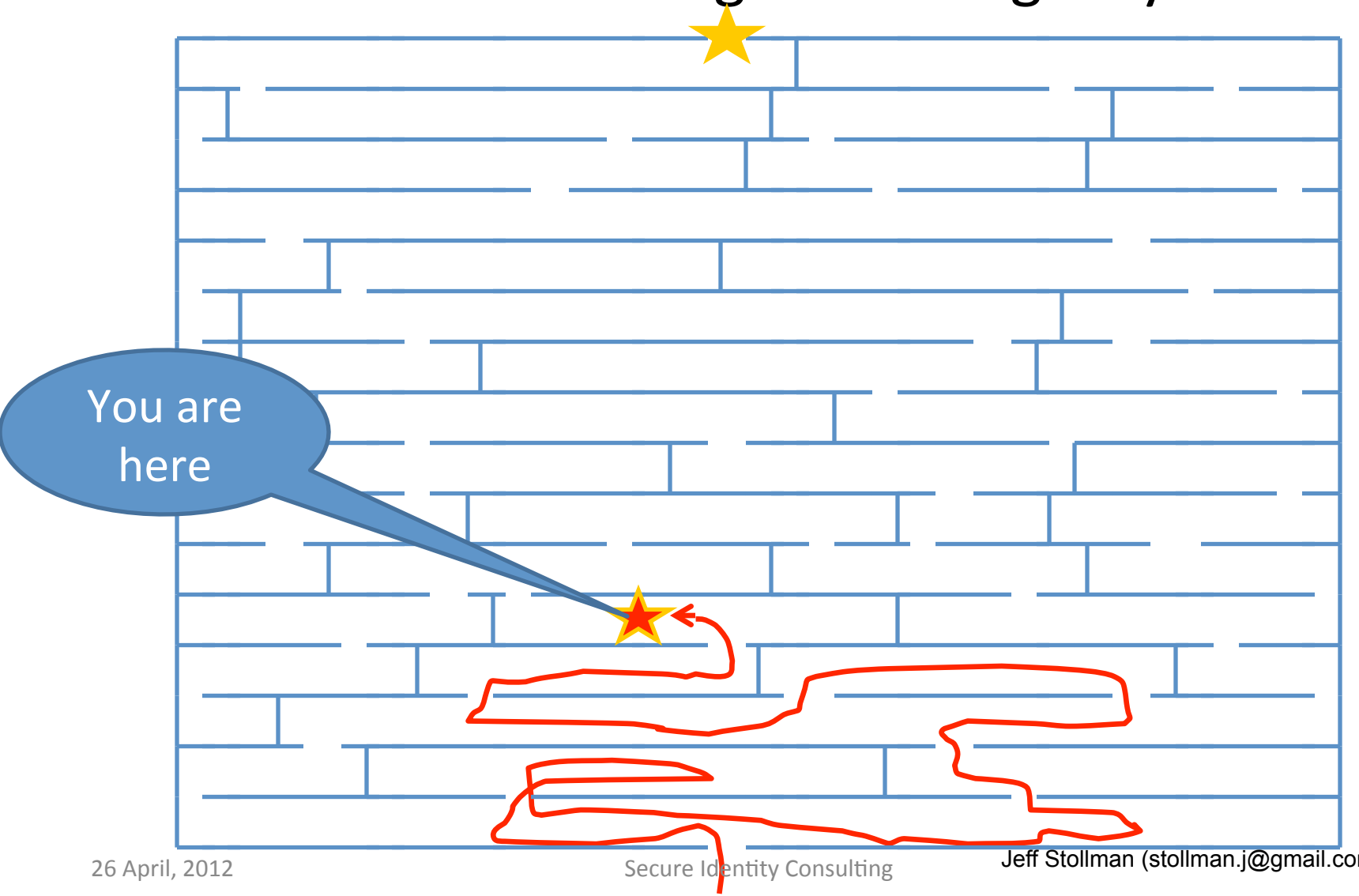
Oops!



The “bottoms-up” empirical model

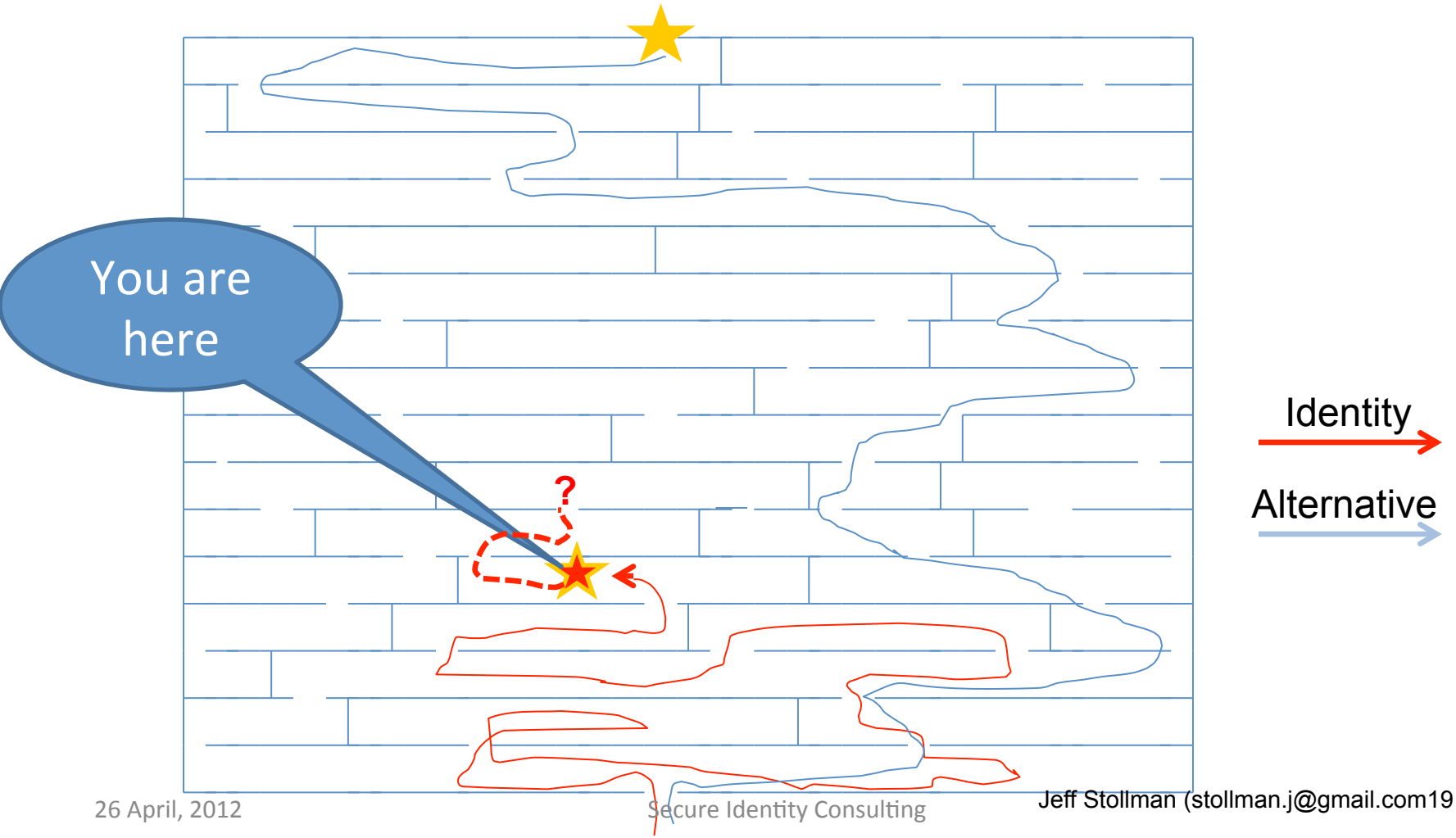
Path to the GPTF

Are we heading the wrong way?

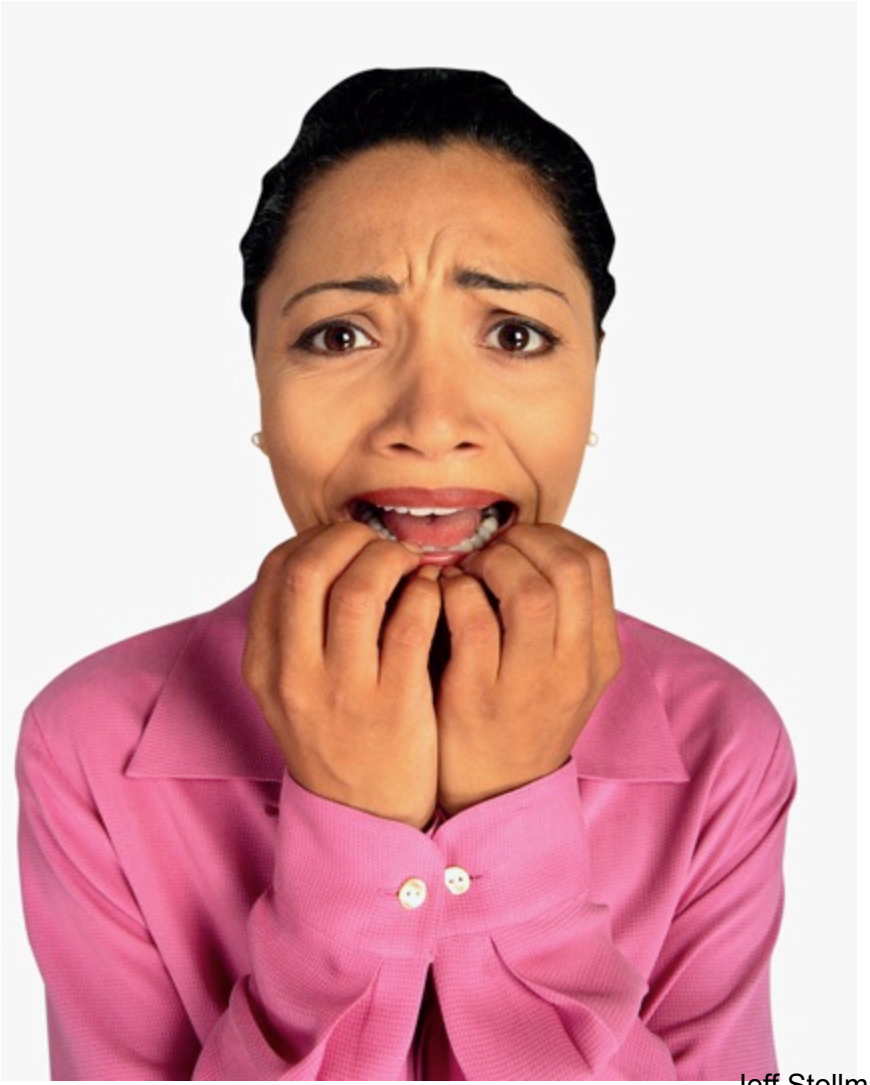


Path to the GPTF

Are we heading the wrong way?



Hope?

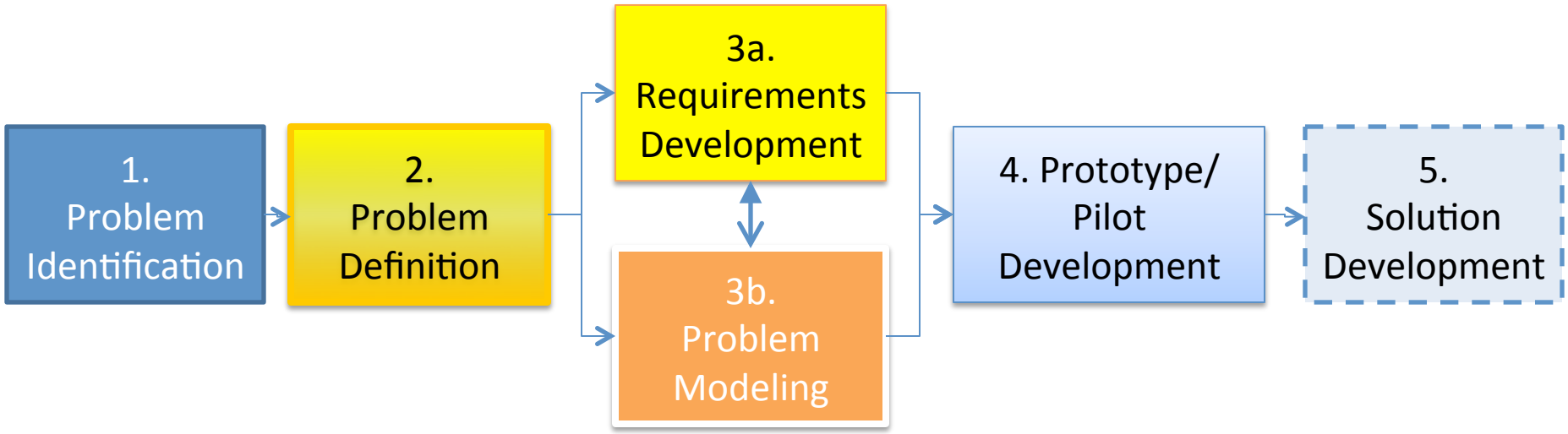


SOLVING THE PROBLEM WITH CERTAINTY

Systems Engineering and the Trust Framework Meta Model

Jeff Stollman (stollman.j@gmail.com21

Systems Engineering Approach

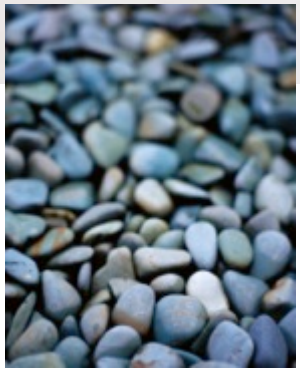


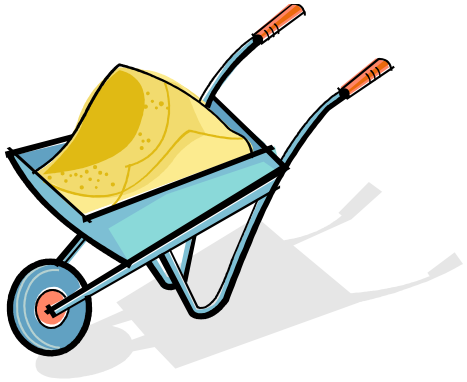
Problem Definition

A problem well-stated is a problem half solved.

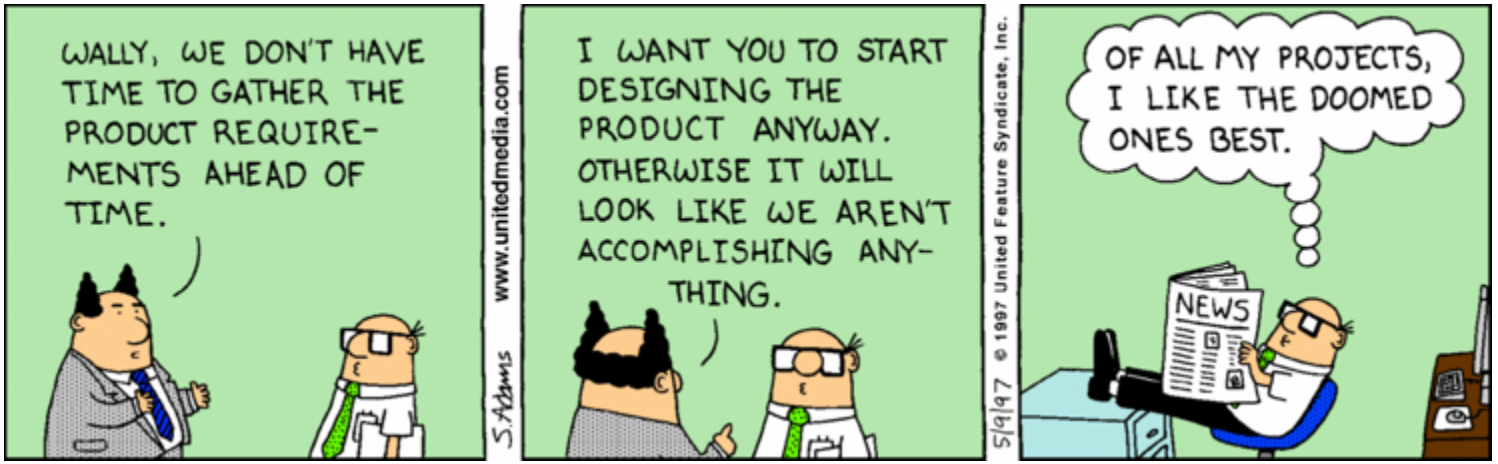
– Charles Kettering, inventor (1876-1958)

Requirements Development





Present Likelihood of Success



Problem Modeling

STEP 2: PROBLEM DEFINITION

Trust

- Oxford English Dictionary definition
  - Firm belief in the reliability, truth, or ability of someone or something

- 1. Firm belief in the reliability, truth, or ability of a counterparty to live up to its duty/commitment
- 2. Willingness (of a party) to engage in a particular interaction

Jeff Stollman (stollman.j@gmail.com28

Trust Element

- 1. A performance commitment by a single party (Object) to a second single party (Subject) that engenders the trust of the Subject in the performance of the Object.
- 2. A consideration of a least one party to a interaction that must be addressed in order to create sufficient trust for the interaction to complete
- E.g.,
  - How has Party B verified that Party A is who s/he claims to be?
  - How will Party C protect my personal information?

Trust Framework

- A set of verifiable commitments from each of the various parties in a transaction to their counter parties.
- These commitments necessarily include
  - Controls (including regulatory and contractual obligations) to help ensure commitments are delivered
  - Remedies for failure to meet such commitments

Trust Framework

- 1. A network of trust relationships among all parties to a transaction that addresses the assurances needed by each of them to trust the other relevant parties for each element of trust
  - It is indivisible.
    - If all trust relationships are not addressed there is the possibility that insufficient trust will exist to facilitate the transaction. Therefore,
  - A viable Trust Framework must be comprehensive.
- 2. A set of verifiable commitments from each of the various parties in a transaction to their counter parties.
  - These commitments necessarily include
    - Controls (including regulatory and contractual obligations) to help ensure commitments are delivered
    - Remedies for failure to meet such commitments

Trust Relationships

- For each trust element, there can be trust relationships between each pair of parties
- Trust relationships are binary
  - i.e., each relationship involves only two parties
- Trust relationships are uni-directional
  - i.e., trust flows only one way in each relationship
  - Mutual trust between two parties for a particular trust element requires two trust relationships
- The potential number of trust relationships in a Trust Framework is the number of permutations (not combinations) of the parties.
  - Not all permutations will be valid for each trust element.

The boundaries of the Trust Framework are established by a matrix of the Parties to the transaction versus the Trust Elements.

STEP 3A: REQUIREMENTS DEFINITION

Requirements Elicitation Process

1. Define Use Cases
2. Model Use Cases
3. Document Requirements for Each Use Case
4. Rationalize Requirements
5. Find Common Requirements

STEP 3B: PROBLEM MODELING

Finding a Vector to Subdivide the Problem

Jeff Stollman (stollman.j@gmail.com36

Finding a Vector To Subdivide the Solution Elements

- Vector must be finite
- Vector must be known
- Vector must be stable throughout a interaction
- Vector must have a small number of elements

Component Vector Candidates

1. Function/Interaction Types
2. Actors
3. Roles
4. Problem Components
5. Trust Elements

Assessment of Function/ Interaction Types

Pros

- Interaction type remains stable over time

Cons

- Potentially infinite
- Not all interaction types are known
- The number of types appears to be quite large.

Assessment of Actors

Pros

- Finite

Cons

- Not all Actors are known
- Actors may change Roles throughout an interaction. They are also likely to serve in multiple roles with different requirements
- The number of types appears to be quite large.

Assessment of Roles

Pros

- Finite
- Actions performed by a Role remain stable

Cons

- Not all Actors are known
- The number of Role types appears to be quite large.

Assessment of Problem Components

Pros

- Trust Elements are finite
- All Trust Elements are known (and have existed for centuries)
- Trust Elements remain stable throughout an interaction
- Five elements may be sufficient to cover all interactions

Cons

Assessment of Trust Elements

Pros

- Trust Elements are finite
- All Trust Elements are known (and have existed for centuries)
- Trust Elements remain stable throughout an interaction
- We propose that five elements may be sufficient to cover all interactions

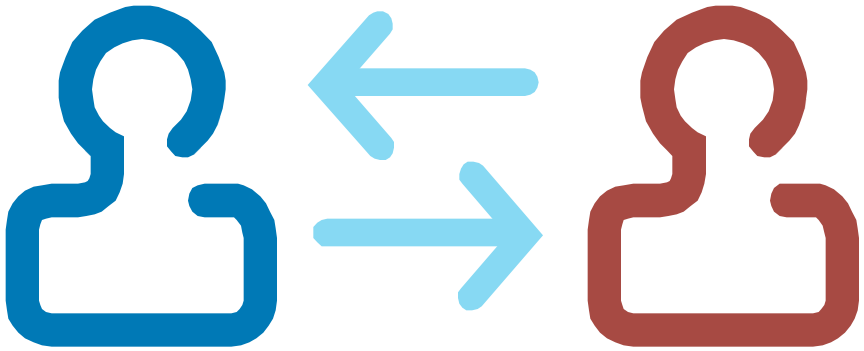
Cons

STEP 3B: PROBLEM MODELING

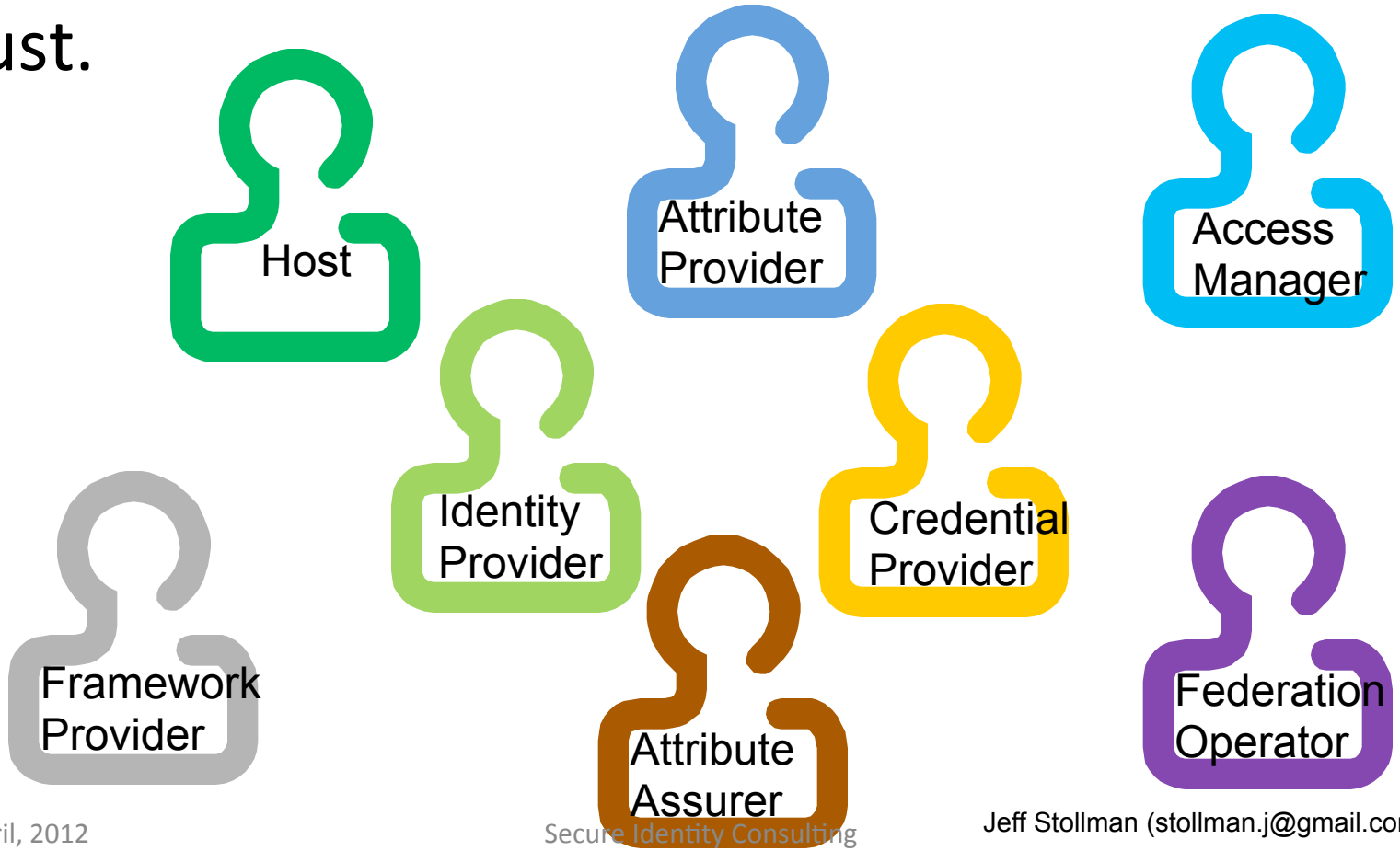
.1 Trust-Element Model

Ultimately, complex interactions emanate from a motivating stimulus that involves only two parties.

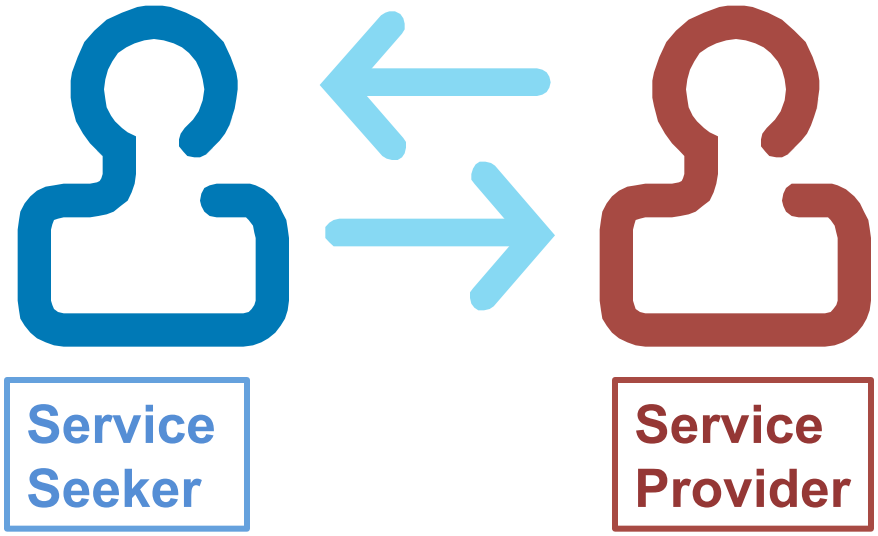
Each party engages in a interaction only when there is sufficient trust in the other to proceed.



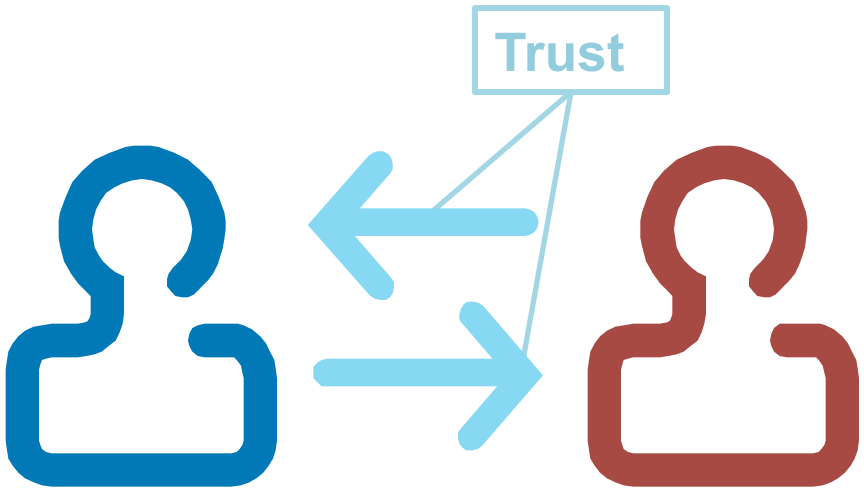
Most of the various other parties that we typically consider vital to the trust/transaction constellation are really all controls invoked by one party or the other to enhance their level of trust.



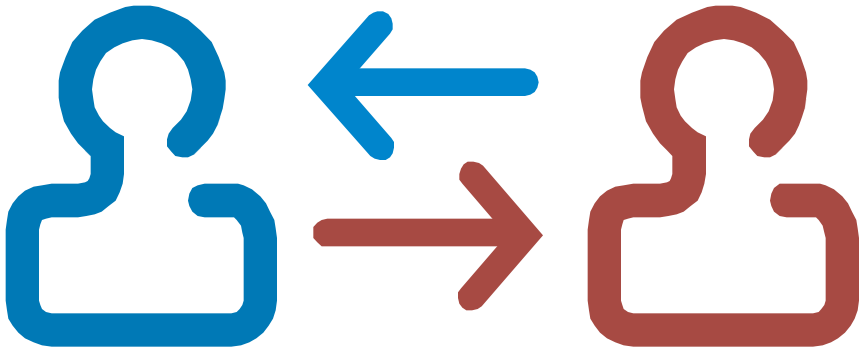
For simplification, we will identify one Party as the Service Seeker and the other as the Service Provider.



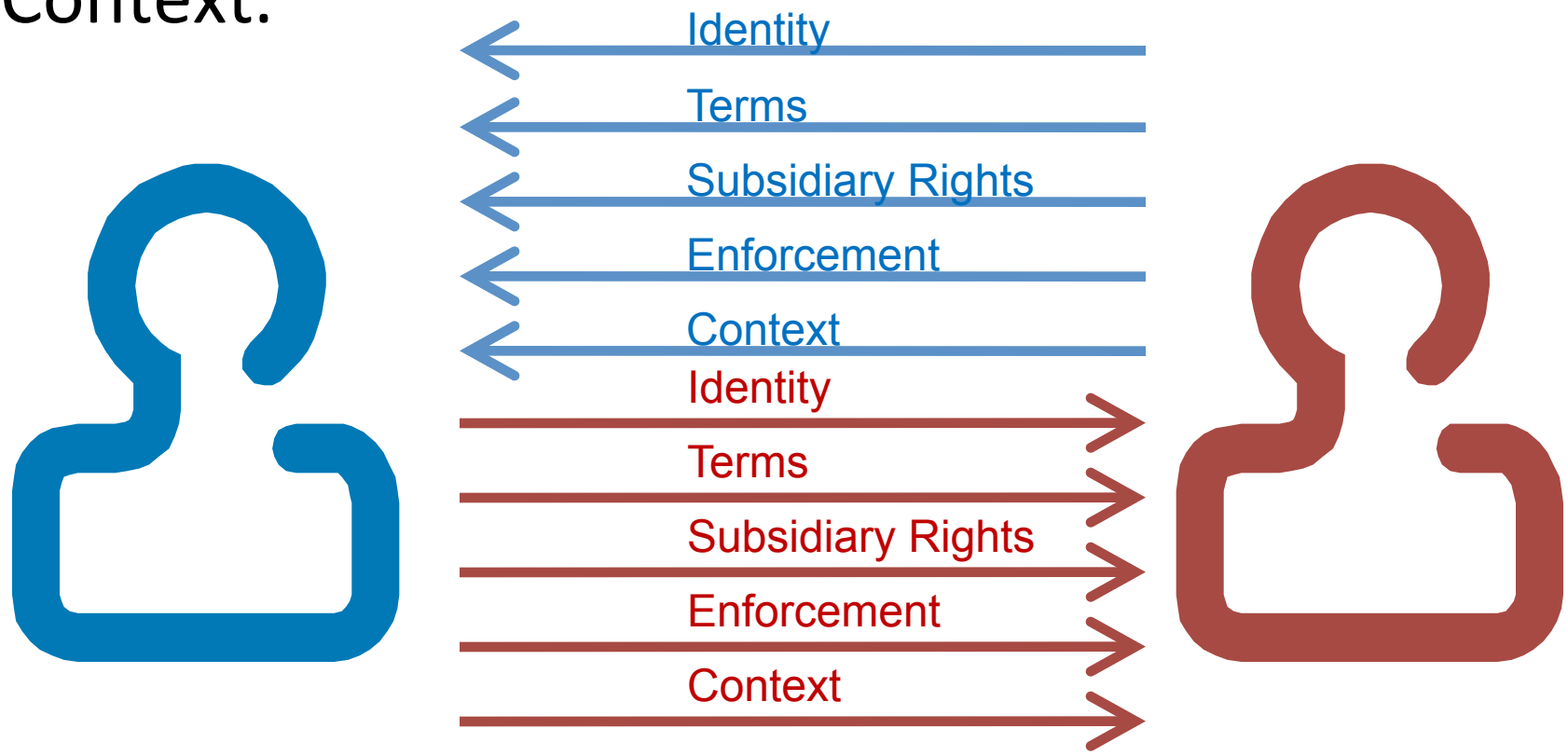
Trust is the confidence each has in the other along several trust vectors. It flows from one party to the other.



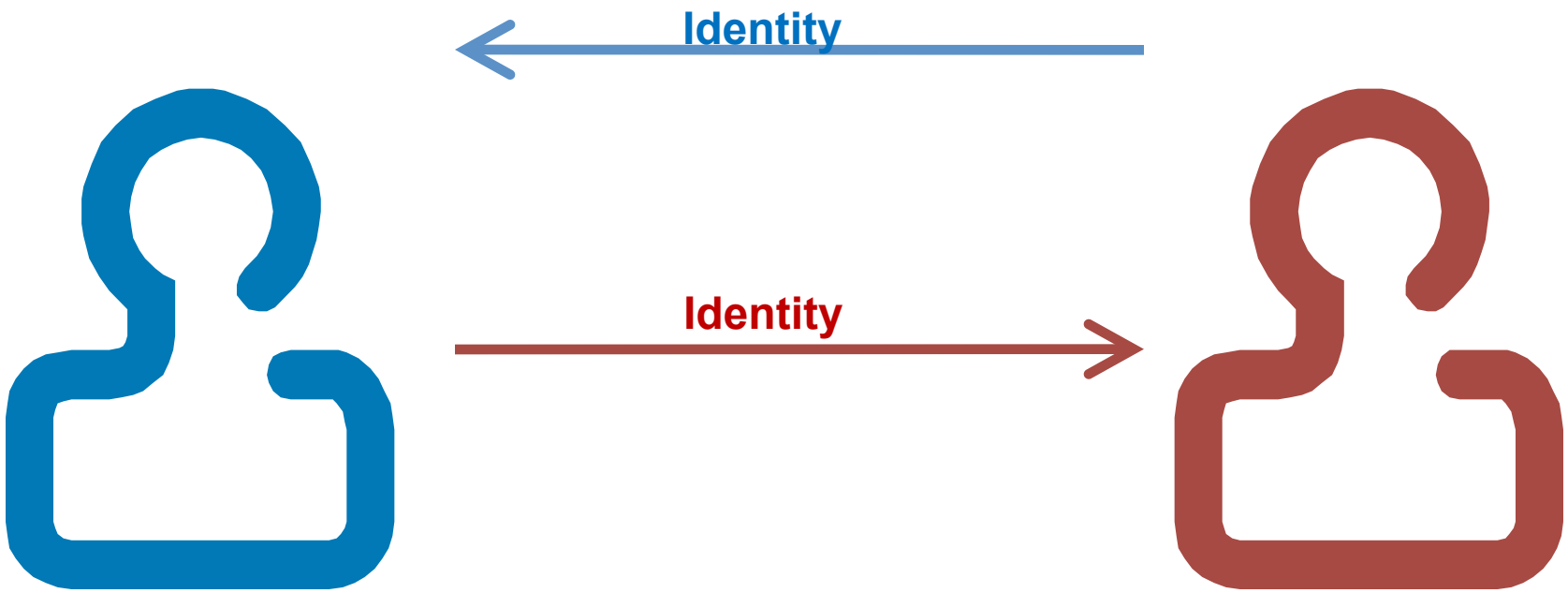
Trust is unidirectional. That is, Party 1 may trust Party 2, but the trust may not be reciprocal. For a transaction to take place, both Parties must trust each other.



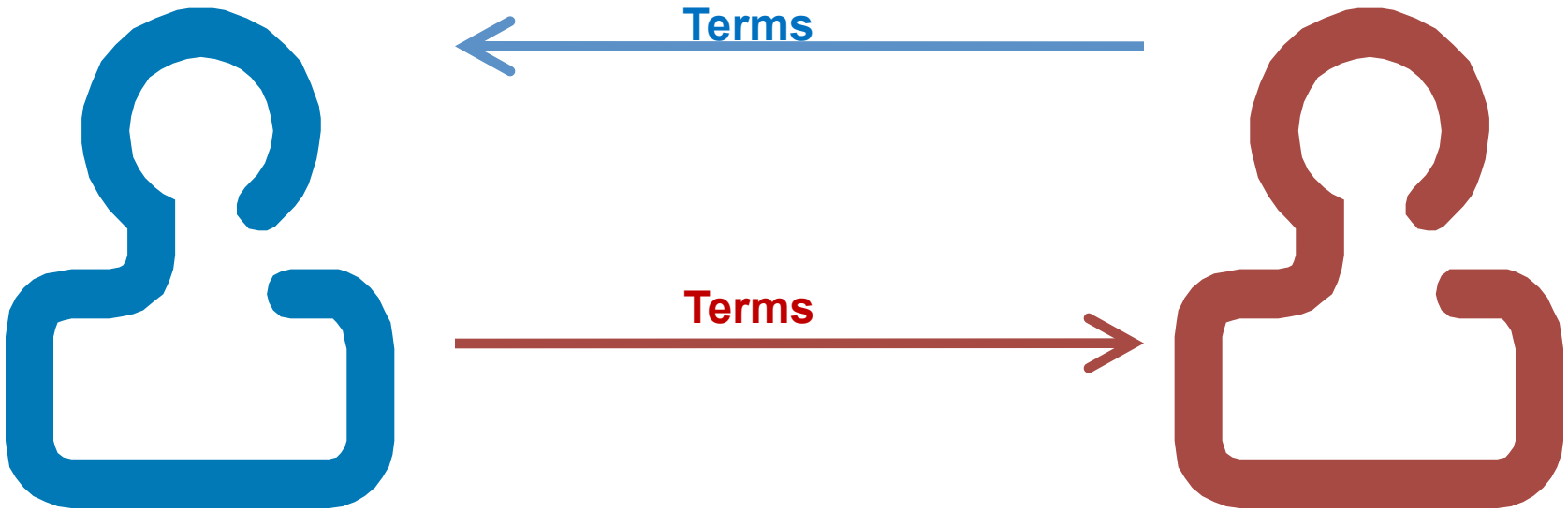
The uni-directional Trust Relationships can be broken down into Trust Components along the five Vectors of Trust: (1) Identity, (2) Terms, (3) Subsidiary Rights, (4) Enforcement, and (5) Context.



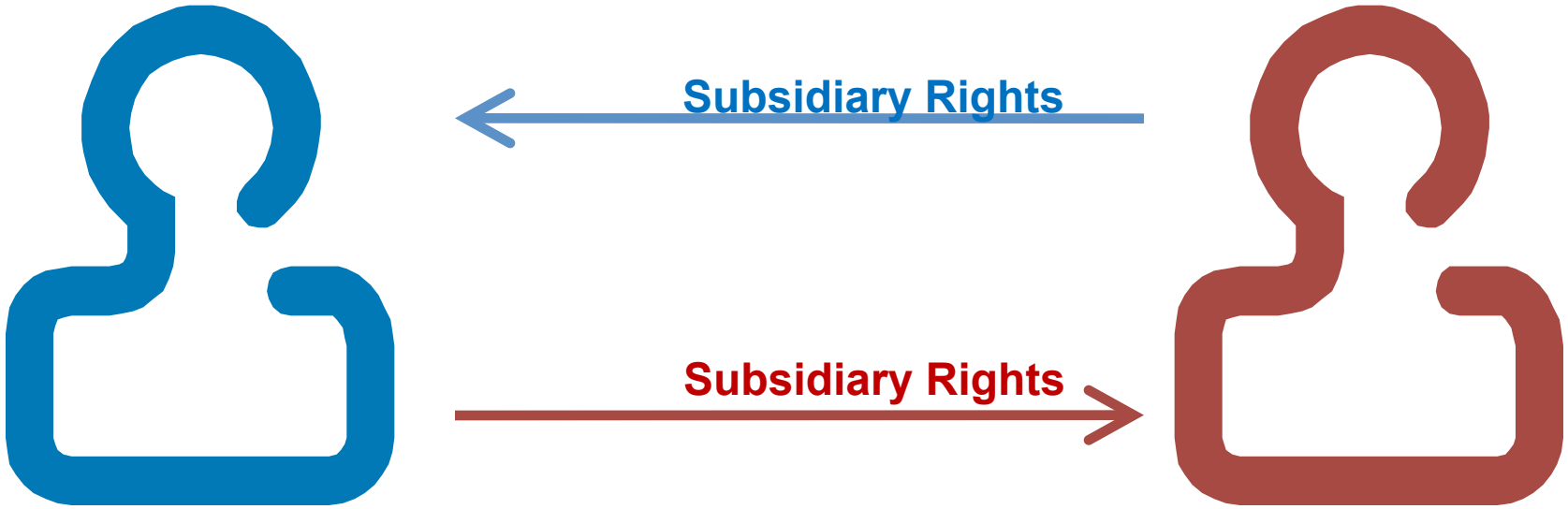
The Identity Trust Component covers the need for each party to understand with whom it is dealing.



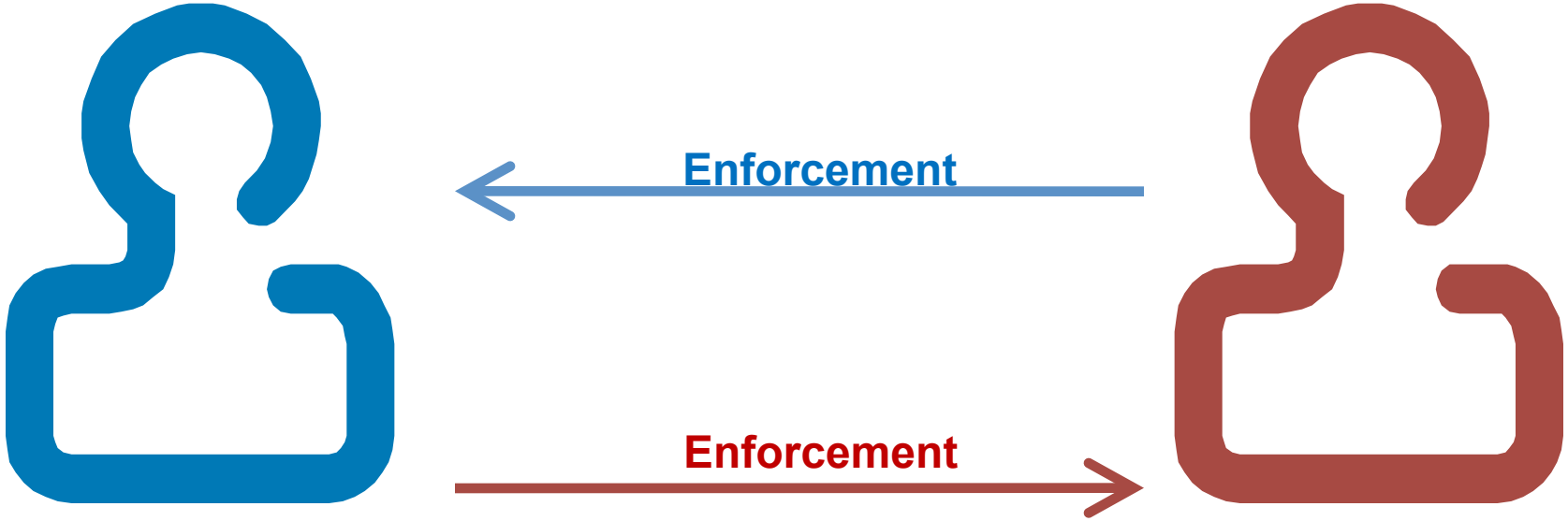
The Terms Trust Component includes both the *advertised* commitments (Service Policies) a Party makes to the counter Party for the transaction, as well as the *demanded* commitments (Terms of Service) sought from the counter Party for the transaction.



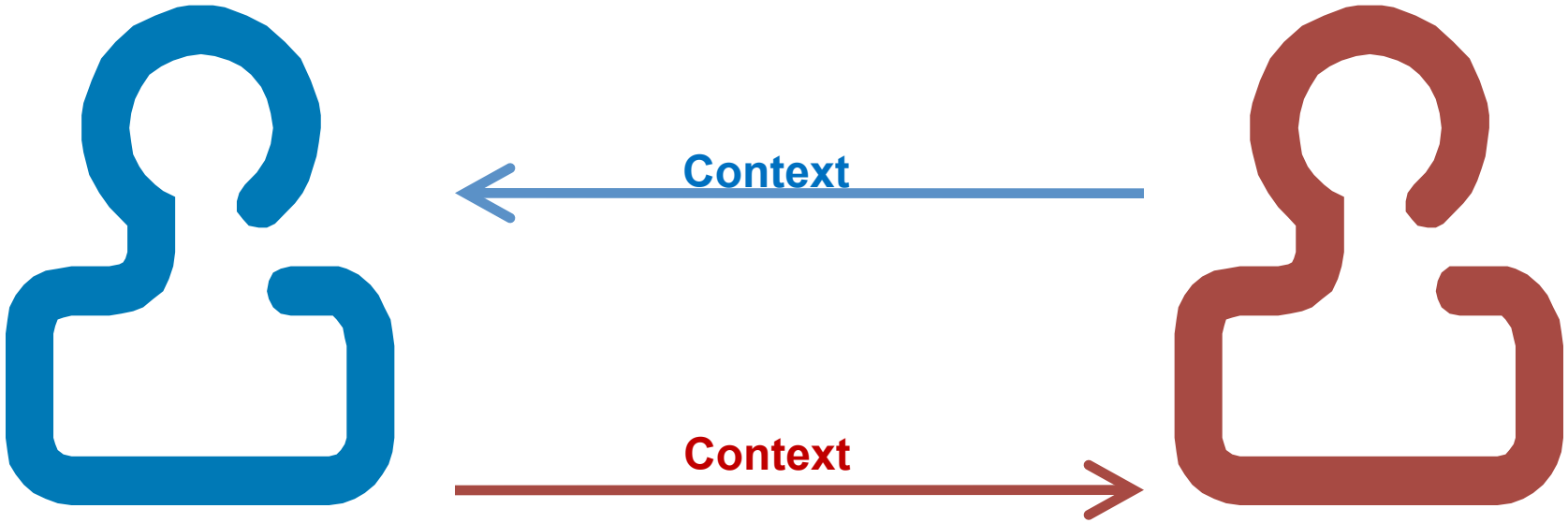
The Subsidiary Rights Trust Component covers the reuse of information accrued during a transaction for other subsequent purposes. This is typically where Privacy Policies come into play.



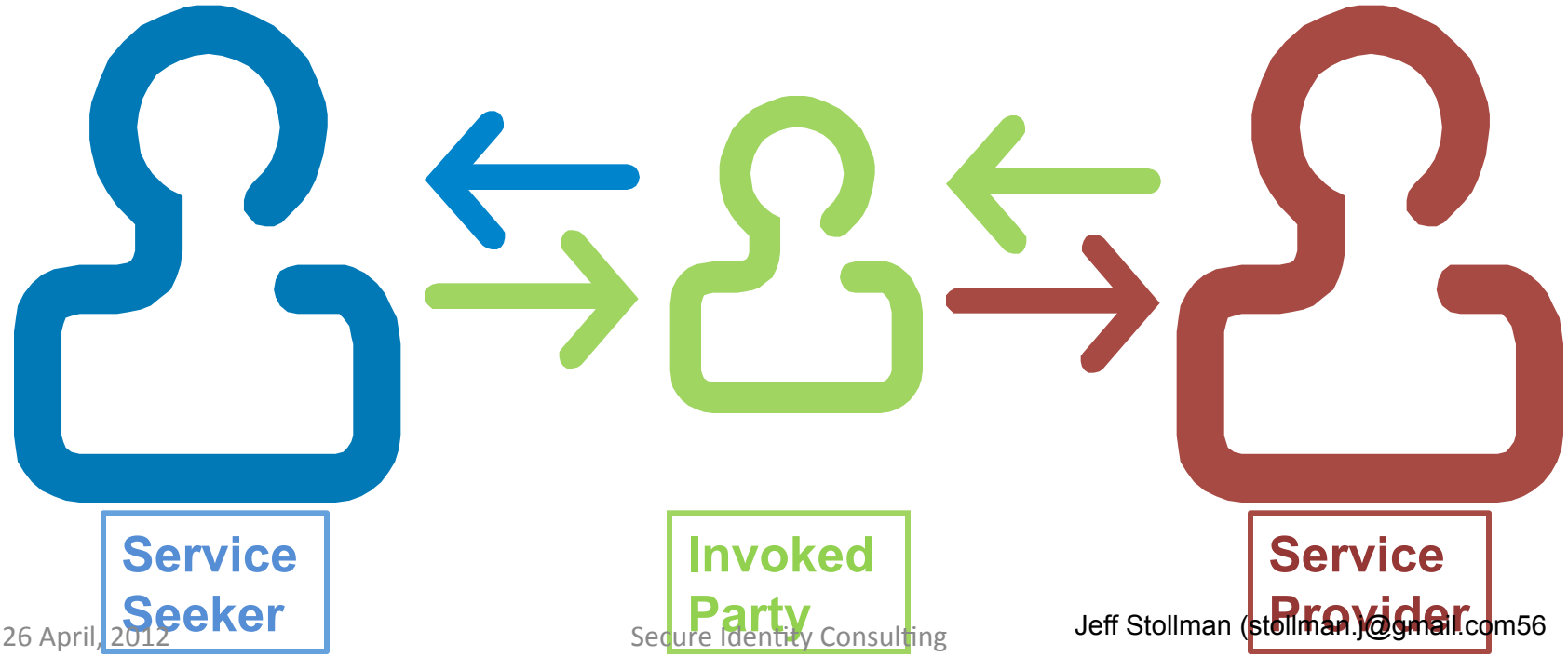
The Enforcement Trust Component includes contracts, regulations, laws, and legal systems (e.g., courts) that can be used to seek redress if transaction commitments from Service Policies and Terms of Service are not adhered to.



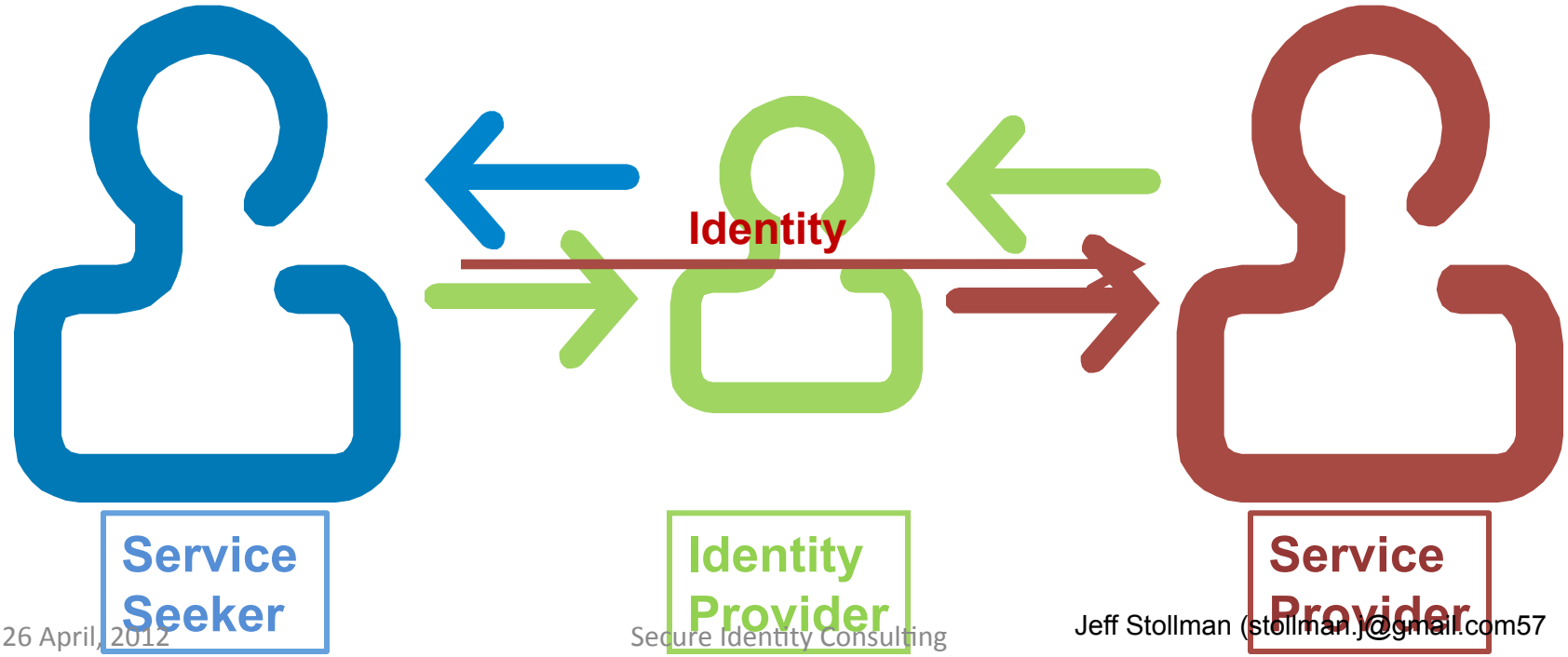
The Context Trust Component includes factors around the transaction. For a face-to-face transaction, parties will need to feel safe and have sufficient privacy to transact. On-line this may translate into session security and integrity.



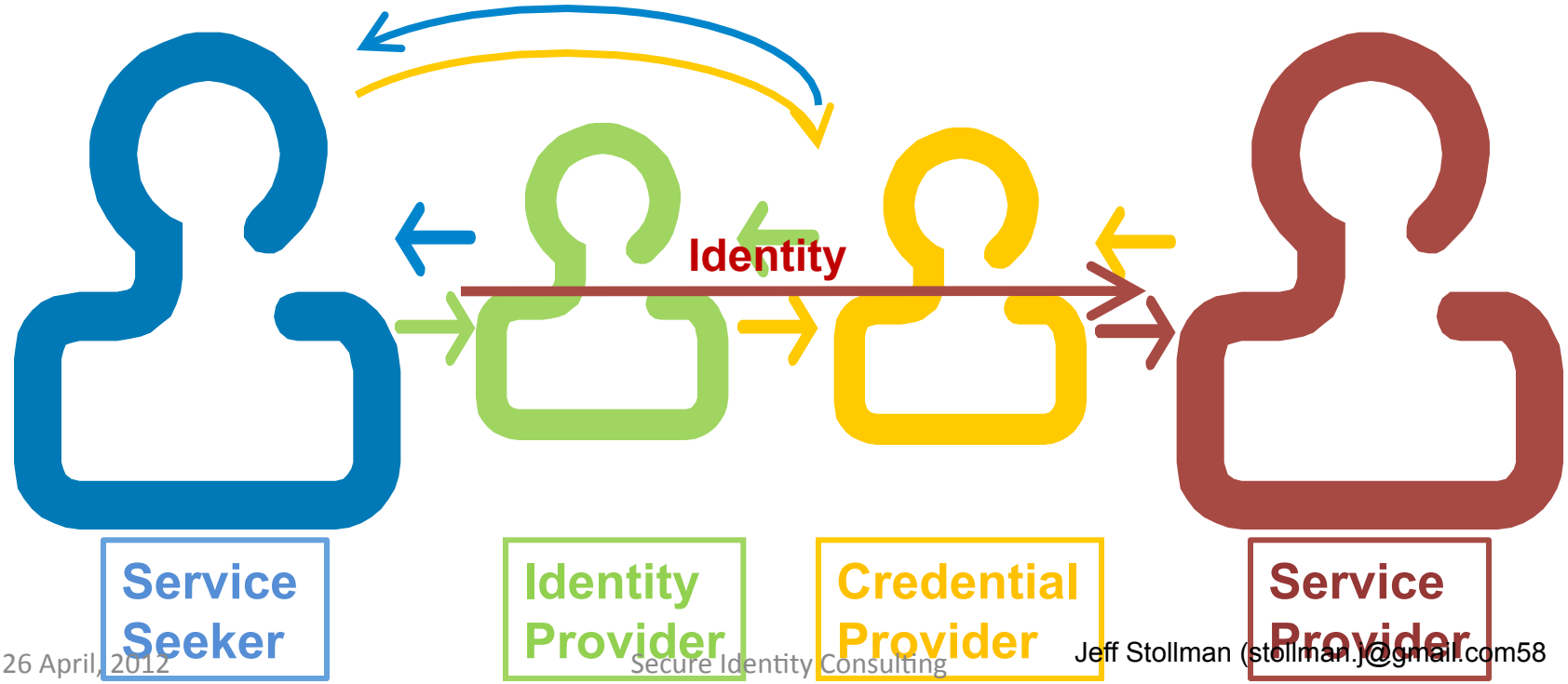
The two primary parties to the transaction may invoke additional parties as controls to enhance their Level of Trust in their counterparties.
The same Trust Components apply to the relationship of the initial Parties to the Invoked Party.



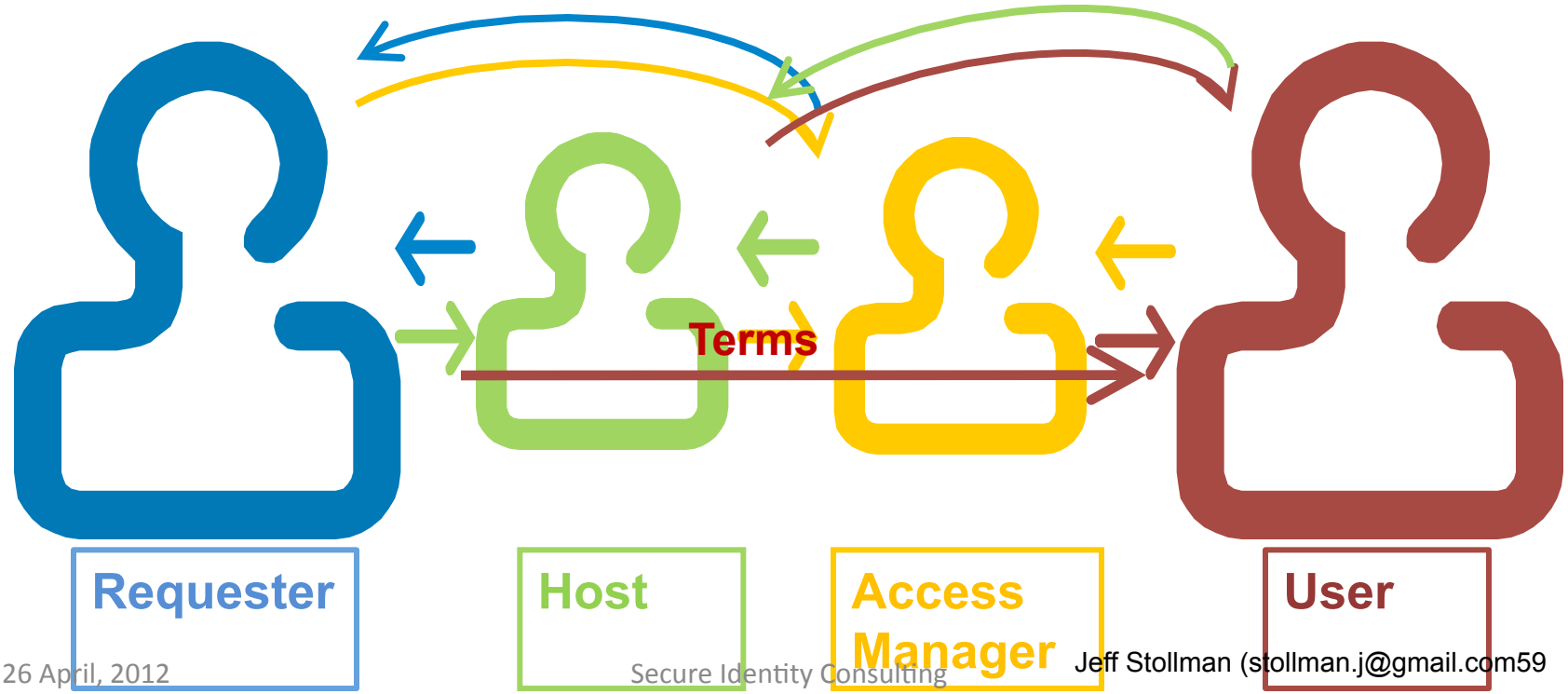
The Service Provider may invoke an Identity Provider to enhance its Level of Assurance in the Identity of the Service Seeker.
This impacts only the Service Provider's leg of the Identity Trust Component.



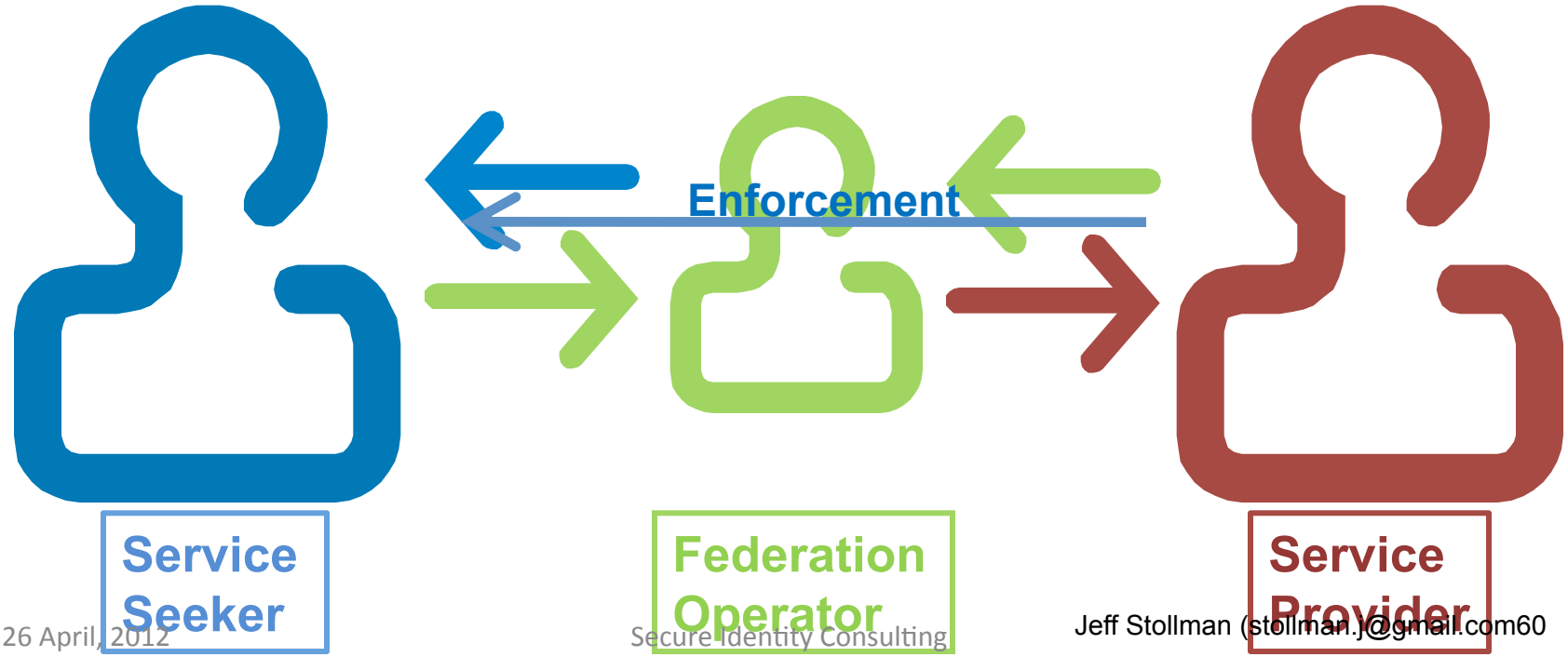
The Service Provider may also invoke an Credential Service Provider as another control to further enhance its Level of Assurance in the Identity of the Service Seeker.



In the UMA model, the Service Provider (User) may also invoke a Host and an Access Manager to further enhance its trust in the Terms Component.

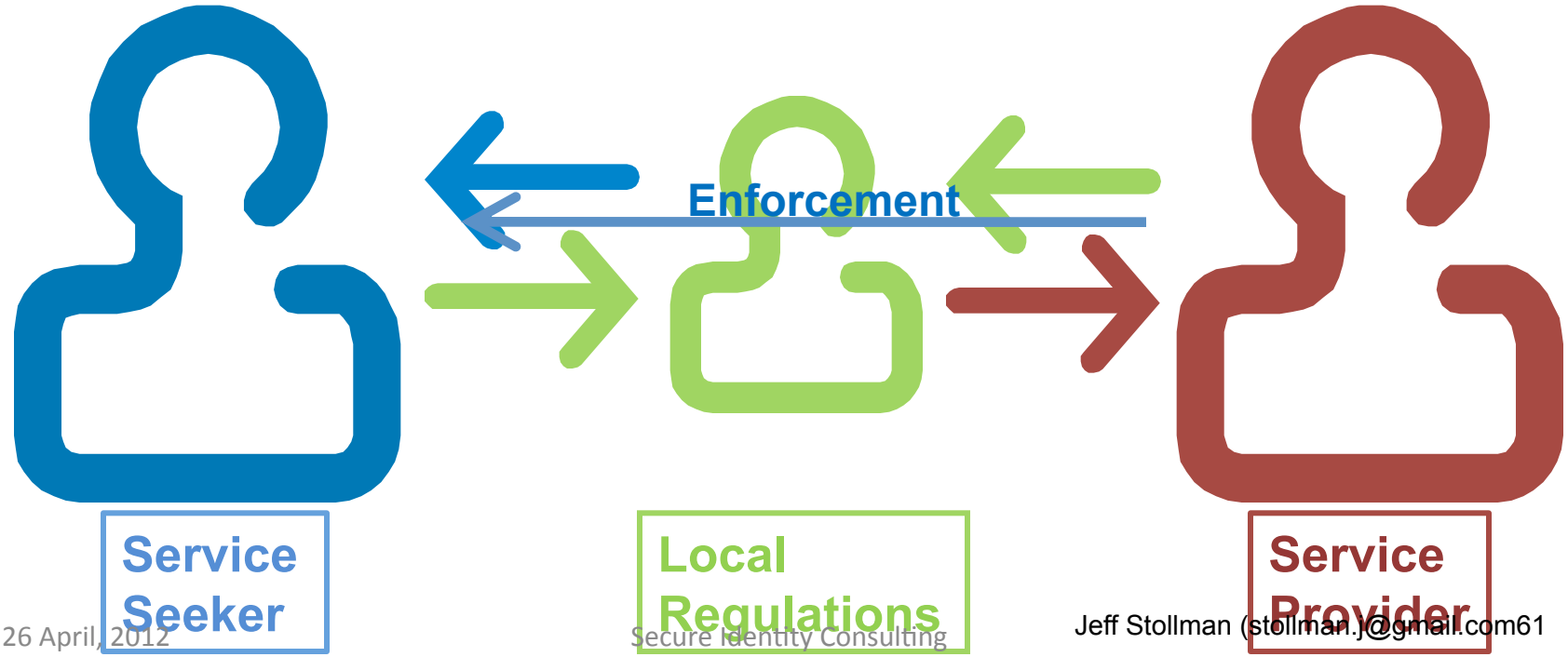


The Service Seeker may invoke the Federation Operator and its rules and remedies for federation members as a control to enhance its Level of Control over the Service Provider.
This impacts only the Service Seeker's leg of the Enforcement Component.



The Service Seeker may invoke Local Regulations as a control to enhance its Level of Control over the Service Provider.

This impacts only the Service Seeker's leg of the Enforcement Component.



STEP 3B: PROBLEM MODELING

.2 Enumerating the trust elements

Trust Element Enumeration Process

1. Identify Trust Relationships by imagining all of the relevant trust issues for each party with all counterparties for all possible use cases.
2. Generalize Trust Relationships into Trust Elements .
   - This allows the same Trust Element to apply to multiple, directional 1->1 relationships among the parties.
   - It avoids generation of a plethora of unique Trust Elements which must be addressed individually.
3. Classify Trust Elements into manageable subsystems

Sample Actual Trust Relationships

1. Alice trusts that the reviews she has heard about the prices and service of WidgetsRUs.com are accurate. (Identity Assurance-Credibility, Controls-Management)
2. Alice trusts that the Privacy Policy published by WidgetsRUs.com is an accurate reflection of their current practices. (Notification)
3. Alice trusts that the user controls described in the Privacy Policy offer her the desired ability to manage her personal information stored by WidgetsRUs.com. (Controls-Subject Controls)
4. Alice trusts that the Privacy Policy advertised by WidgetsRUs.com is an accurate reflection of their future practices. (Notification)
5. Alice trusts that the business practices used by WidgetsRUs.com are above board, legal, and ethical. (Identity Assurance-Credibility)

Example Generalized Trust Elements

- Identity Proofing
- Credential Issuance
- Data Collection 1
- Data Collection 2
- Data Protection 3

- Comprehensiveness of process used to verify that a Subject is who he/she/it represents itself to be to Object
- Robustness (resistance to counterfeiting) of process of credential issuance to Subject by Object
- Extent of risk imposed on Subject through the data collected by Object
- Extent to which Object collects only the minimum amount of data from Subject needed to support transaction
- Ease with which Subject can exercise control over release of personal information by Object

Speculation

- It is commonly assumed that our Service Assessment Criteria must follow existing regulatory requirements.
- I suggest that this is not so.
- If we devise reasonable Service Assessment Criteria that afford multiple levels of assurance/protection for each subsystem, entities can seek certification at the level needed to meet both their business and regulatory requirements.
- Hopefully, the Criteria levels will afford enough parallelism with major regulations to make this achievable.
- If not, perhaps the maturity of our framework will prompt regulators to have the courage to update their codes, coalescing around a better mix of economy and protection.

Jeff Stollman (stollman.j@gmail.com66

NEXT STEPS

Conclusions

1. The Trust Framework already exists; it merely needs to be articulated.
2. The Trust Framework problem is a System-of-Systems problem, i.e., it consists of several subsystems that are interdependent.
3. The Trust Framework defines a comprehensive "web of trust" that includes a large number of interrelated Trust Elements that are of importance to at least one Party in the range of transactions (use cases) conducted under the Trust Framework.

Conclusions cont'd.

4. The Trust Elements are the requirements for any attempt at implementing solutions that seek to provide trust.
5. While, in an ideal world, solutions are needed for each Trust Element in this multi-dimensional matrix, in order to afford sufficient trust for all parties to willingly participate, practical levels of trust can be obtained by specifying criteria for selective cells.

Conclusions cont'd.

6. By attaining consensus on the map of the problem space (the Trust Elements and the Parties/Roles), we can determine the appropriate categories for major subsystems (e.g., Identity, Privacy, Notification, Management, Controls).
7. After attaining consensus, we can allocate the cells among the sub-systems to allow us to work in parallel to more rapidly build a coherent Trust Framework.
8. We can prioritize the order in which we address the cells to maximize our impact.

Conclusions cont'd.

9. As long as we follow the map, we can shift cells from subsystem to subsystem and reprioritize the order without losing coherence.
10. Implementing solutions to address a subset of Trust Elements without understanding the entire framework and its System-of-Systems requirements, runs the risk that the solutions will violate these requirements and create an untenable morass such as the conflicting jurisdictional regulations we face today.

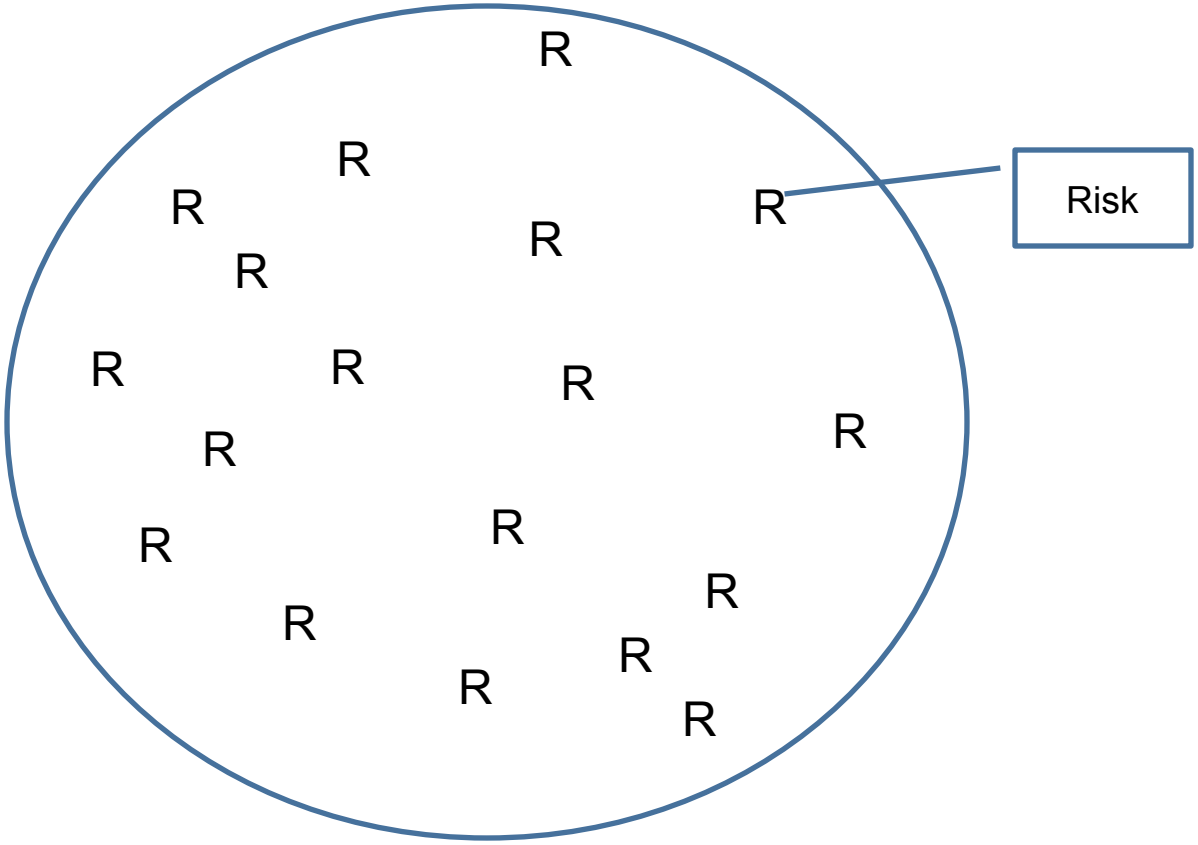
Where do we go from here?

- Funding is needed to conduct Steps 2, 3a & 3b
- Funding is unlikely to come from industry – there is no return on investment
- Fund should come from government in order to pave the way for commercial development
  - The Trust Framework Meta Model is vital infrastructure that is needed to facilitate the development and deployment of usable trust frameworks

BACKUP SLIDES

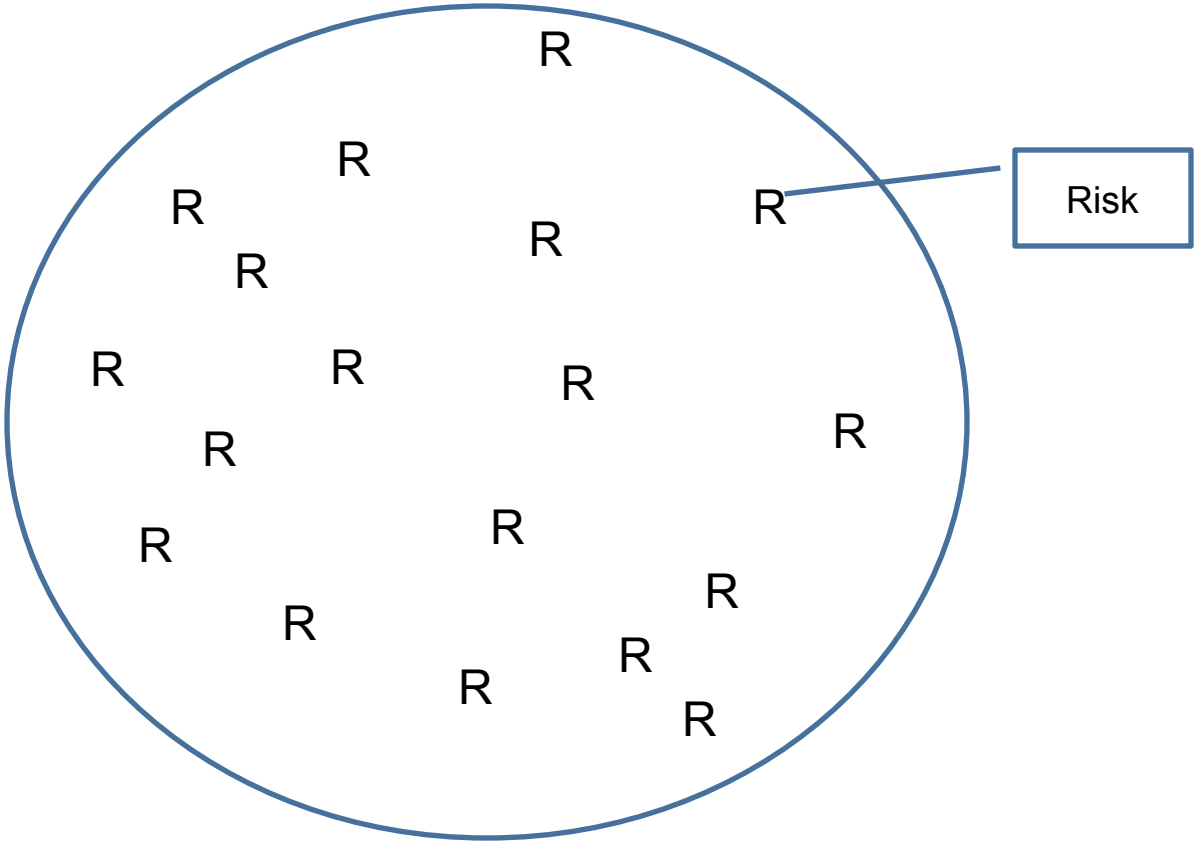
RISK-BASED MODEL

Risk-Based Model

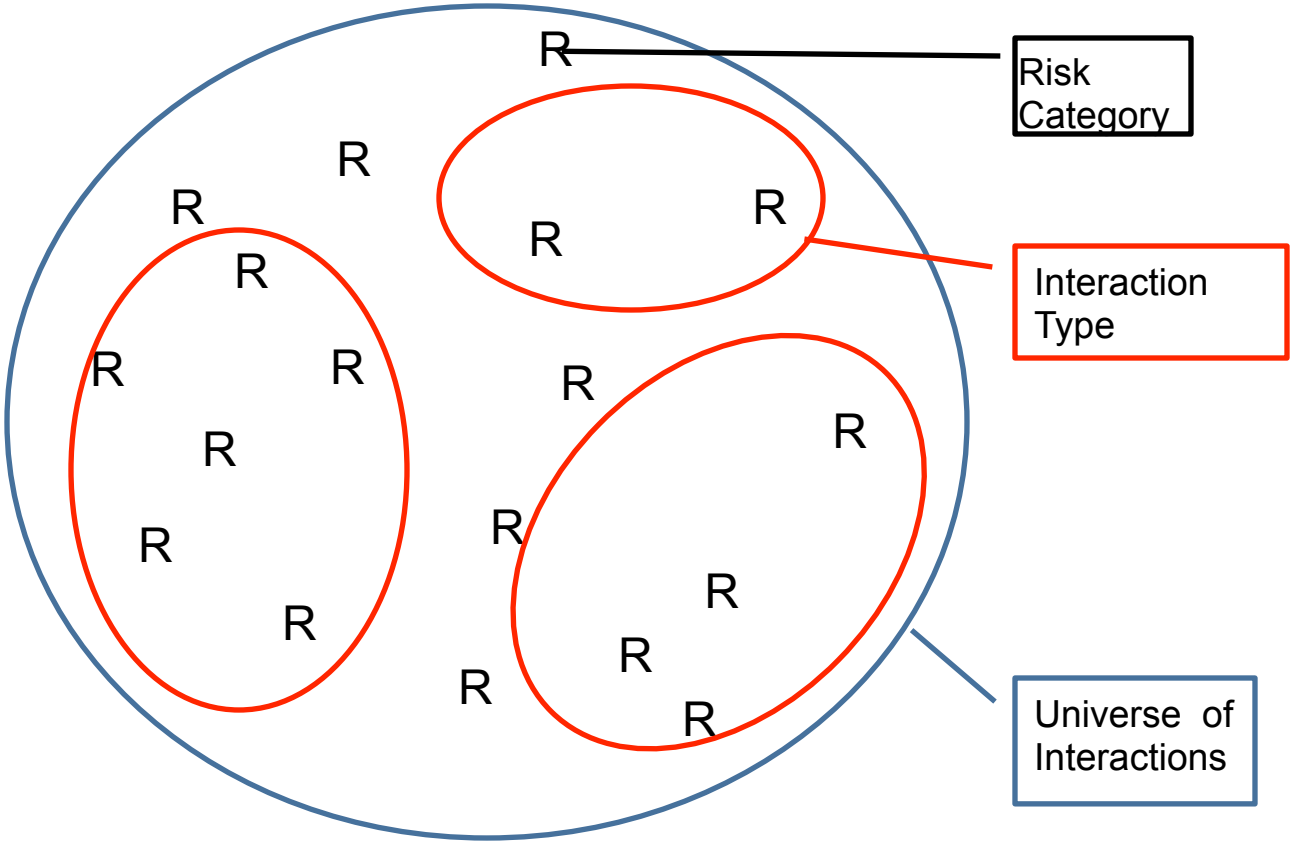


Jeff Stollman (stollman.j@gmail.com75

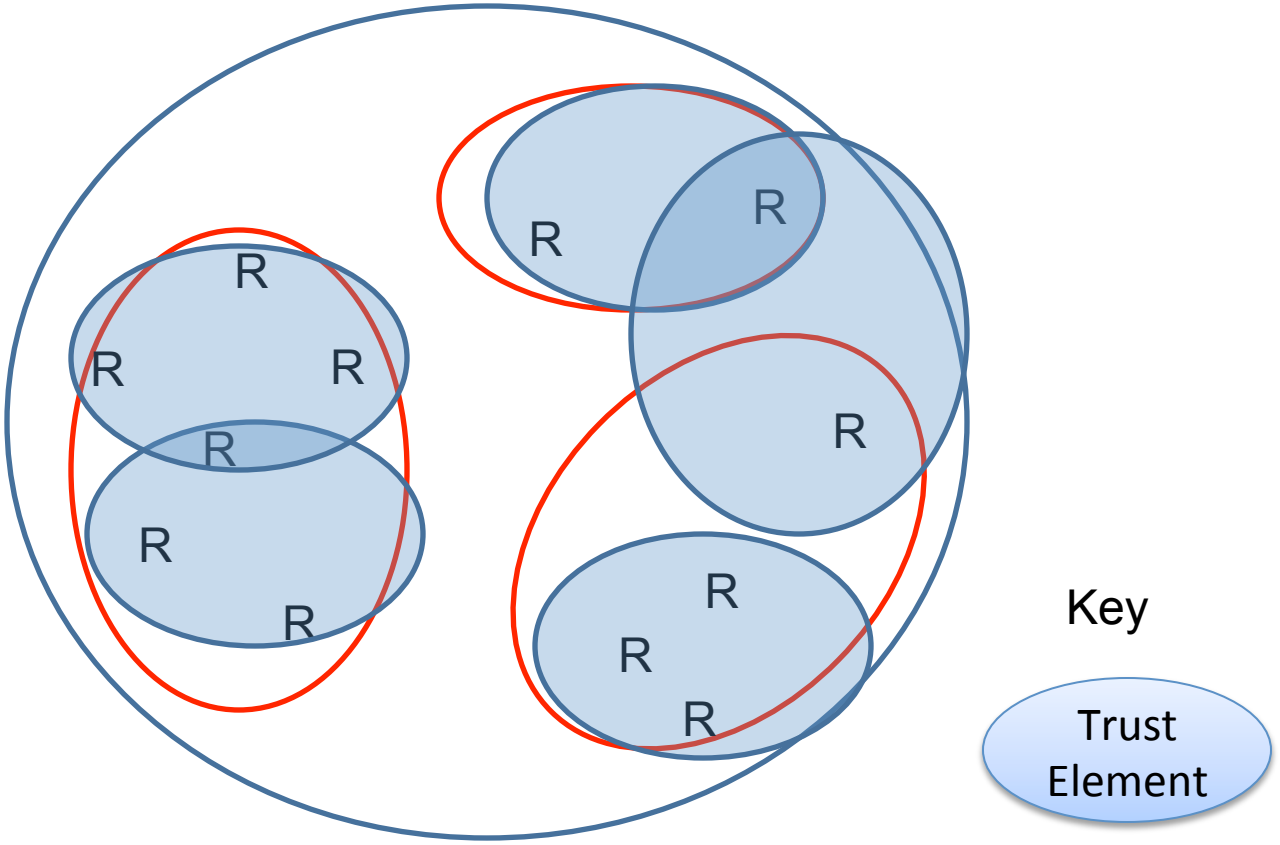
Risk-Based Model: Risks



Risk-Based Model: Trust Elements

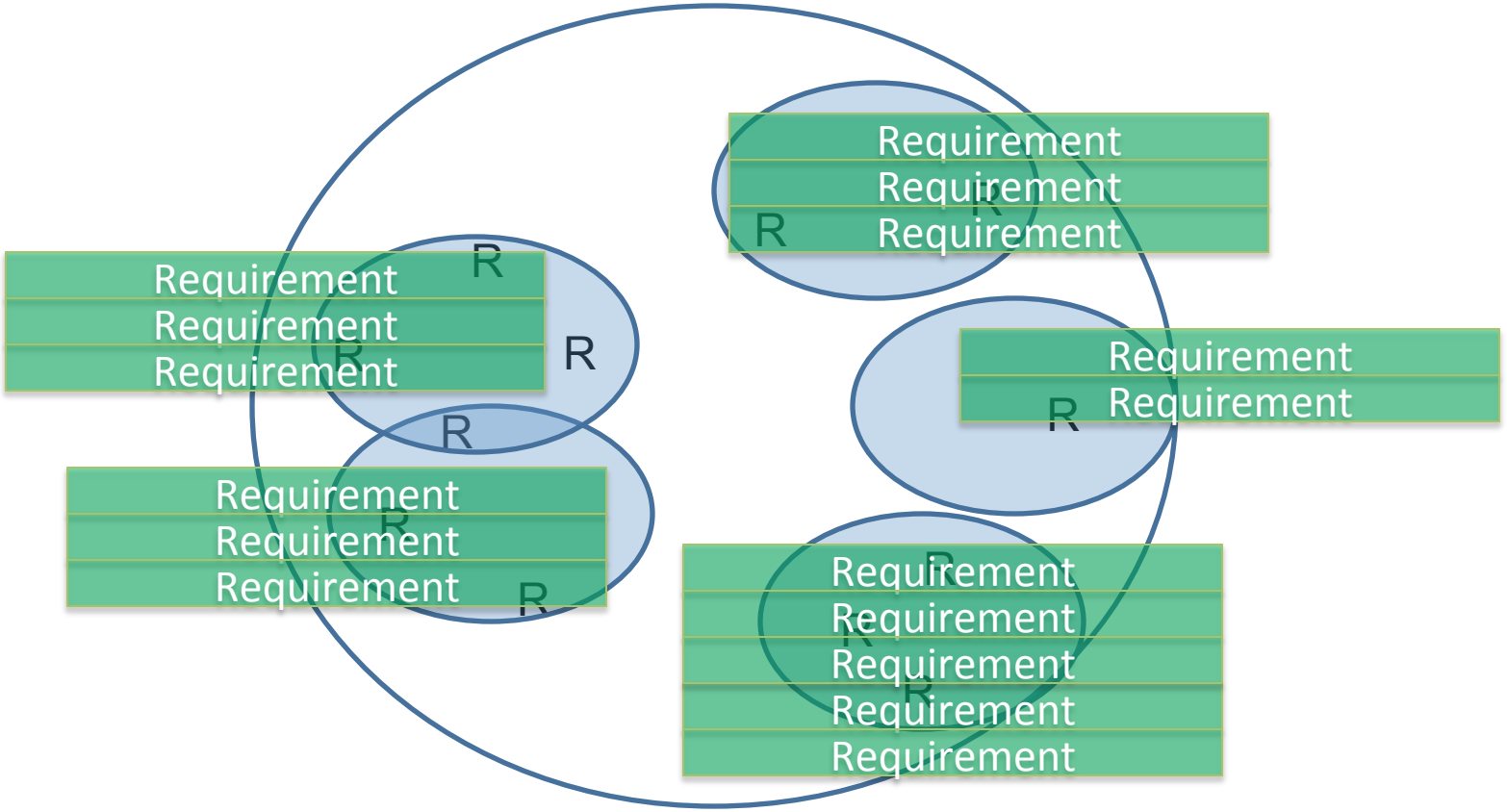


Risk-Based Model: Trust Elements



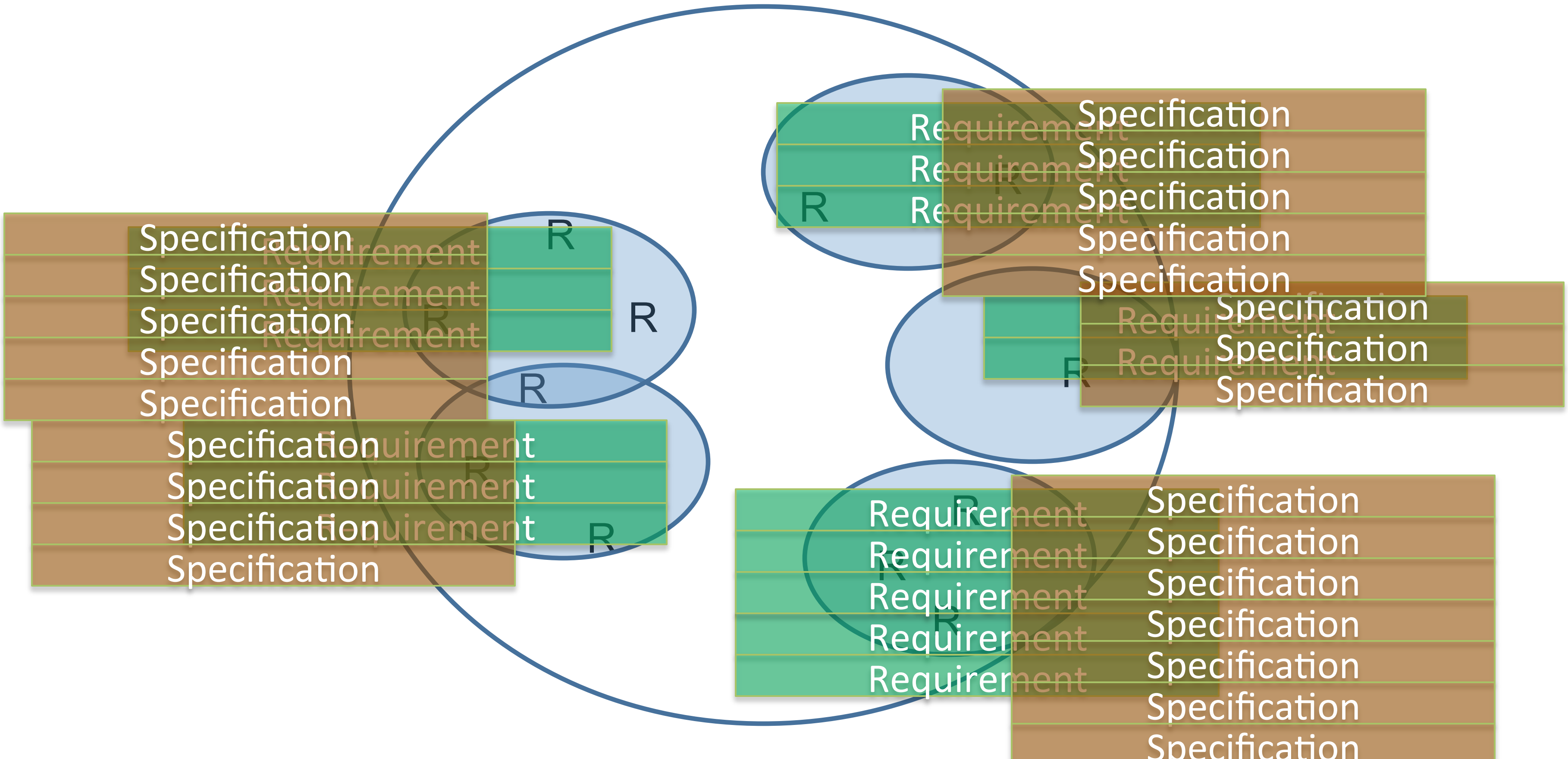
Jeff Stollman (stollman.j@gmail.com78

Risk-Based Model: Requirements

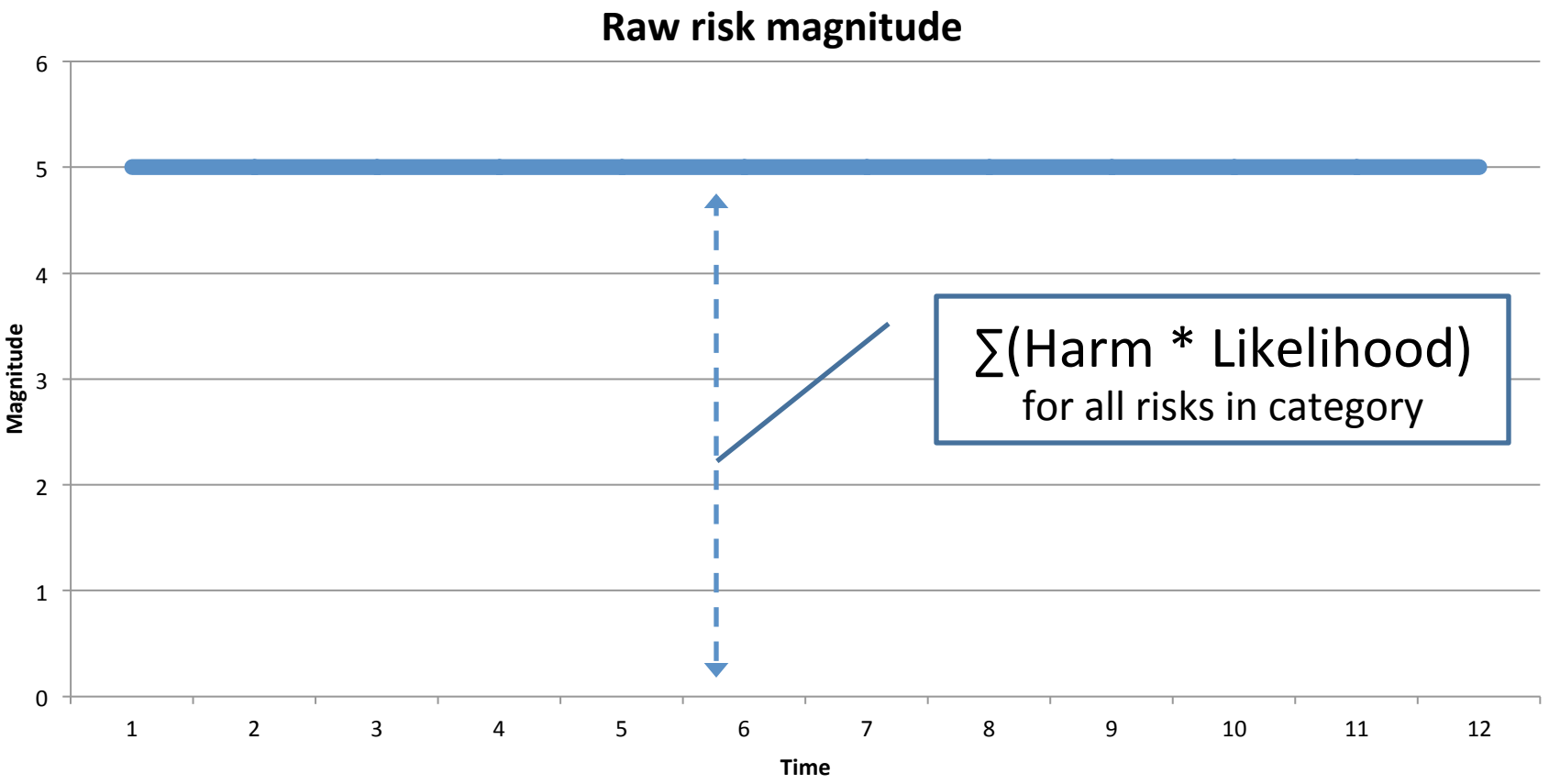


Jeff Stollman (stollman.j@gmail.com79

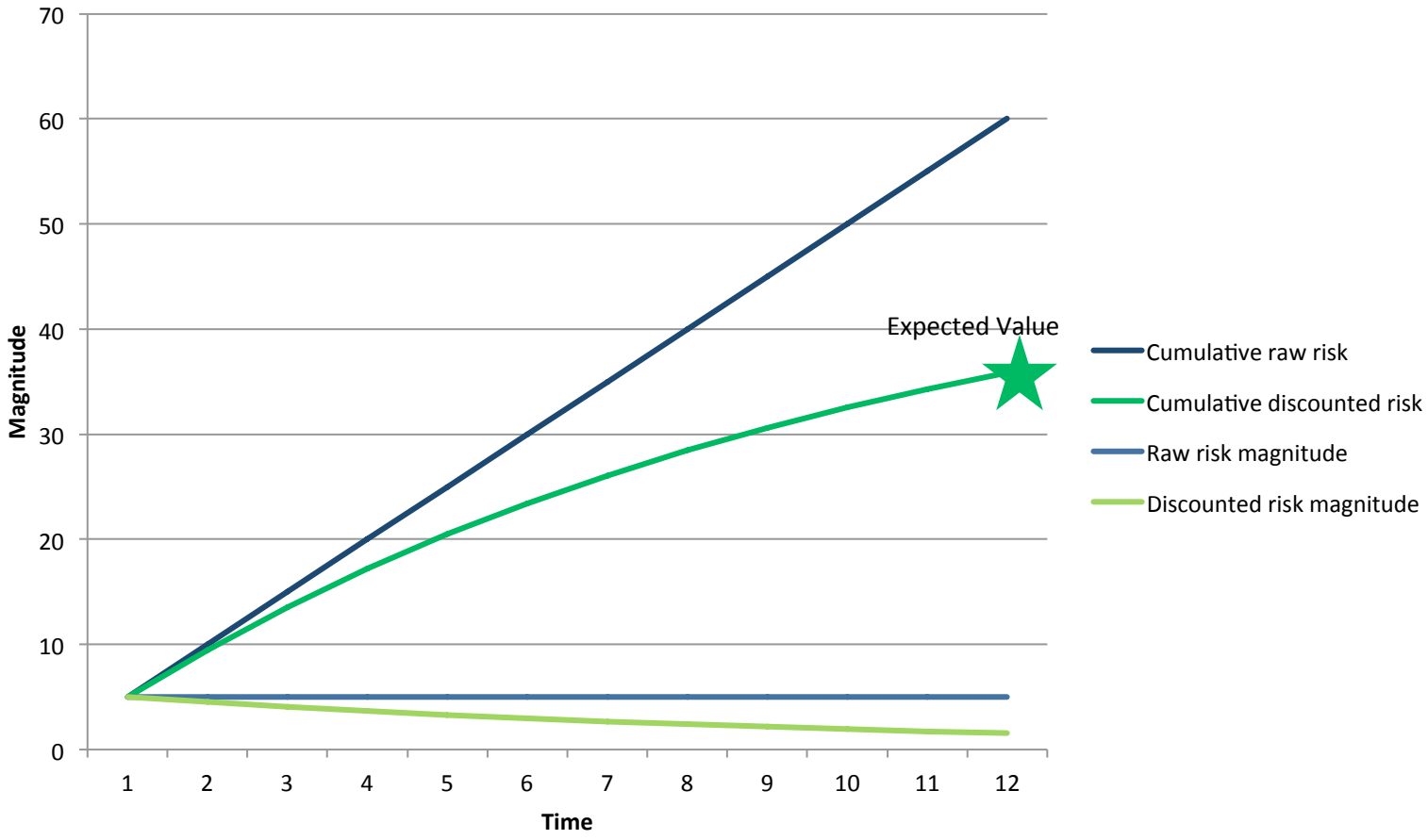
Risk-Based Model: Specifications



Quantifying Risk 1



Quantifying Risk 2



Jeff Stollman (stollman.j@gmail.com82

Definitions

- IPSEITY
  - Your unique carbon life form
- ATTRIBUTE
  - All information (claims/assertions) about an entity that is not Ipseity