
# Infrastructure for Trusted Computing

## Briefing to ACSAC
## December 7, 2004

# Contents

- **The Challenge of Trusted Computing**
- The Trusted Platform Lifecycle
- Model for Infrastructure
- Model for Platform Authentication
- Use Case: End-Point Integrity
- Summary

TRUSTED COMPUTING GROUP™

# The Challenge of Trusted Computing

- Trusted Computing
  - How to create a safer computing environment that is faced with increasing frequency and sophistication of attacks
  - Protect end-user data
  - Enable trusted eCommerce transactions
  - Hardware-rooted trust
- Increase the level of trust in the PC platform
  - Increase consumer confidence in Internet use
  - Reduce business risks, specially for security-conscious sectors
    - Financial Services, Insurance, Government, Healthcare
  - Increase in transaction volume and value with hardware enforced protections
- Increase trust in other platforms
  - Laptops, Desktops, PDA, Servers, Mobile Phones, Network gear, etc.

TRUSTED COMPUTING GROUP™

# "Infrastructures for Trust"

- Trusted Computing (TC): meeting point of Social Trust and Technical Trust
  - Social Trust: based on business & legal relationships marketing & perception, history, etc.
  - Technical Trust: "*An entity can be trusted if it always behaves in the expected manner for the intended purpose*"
    - Feed-back relationship
- Broader meaning of "Infrastructure:
  - Trust in products from manufacturers (Pre-deployment)

    → How do I know this machine has so and so HW/SW
  - User's trust in each other's machines (Deployment)

    → How does Alice know that Bob is using a "safe" platform

TRUSTED COMPUTING GROUP™

# Contents

- The Challenge of Trusted Computing
- **The Trusted Platform Lifecycle**
- Model for Infrastructure
- Model for Platform Authentication
- Use Case: End-Point Integrity
- Summary

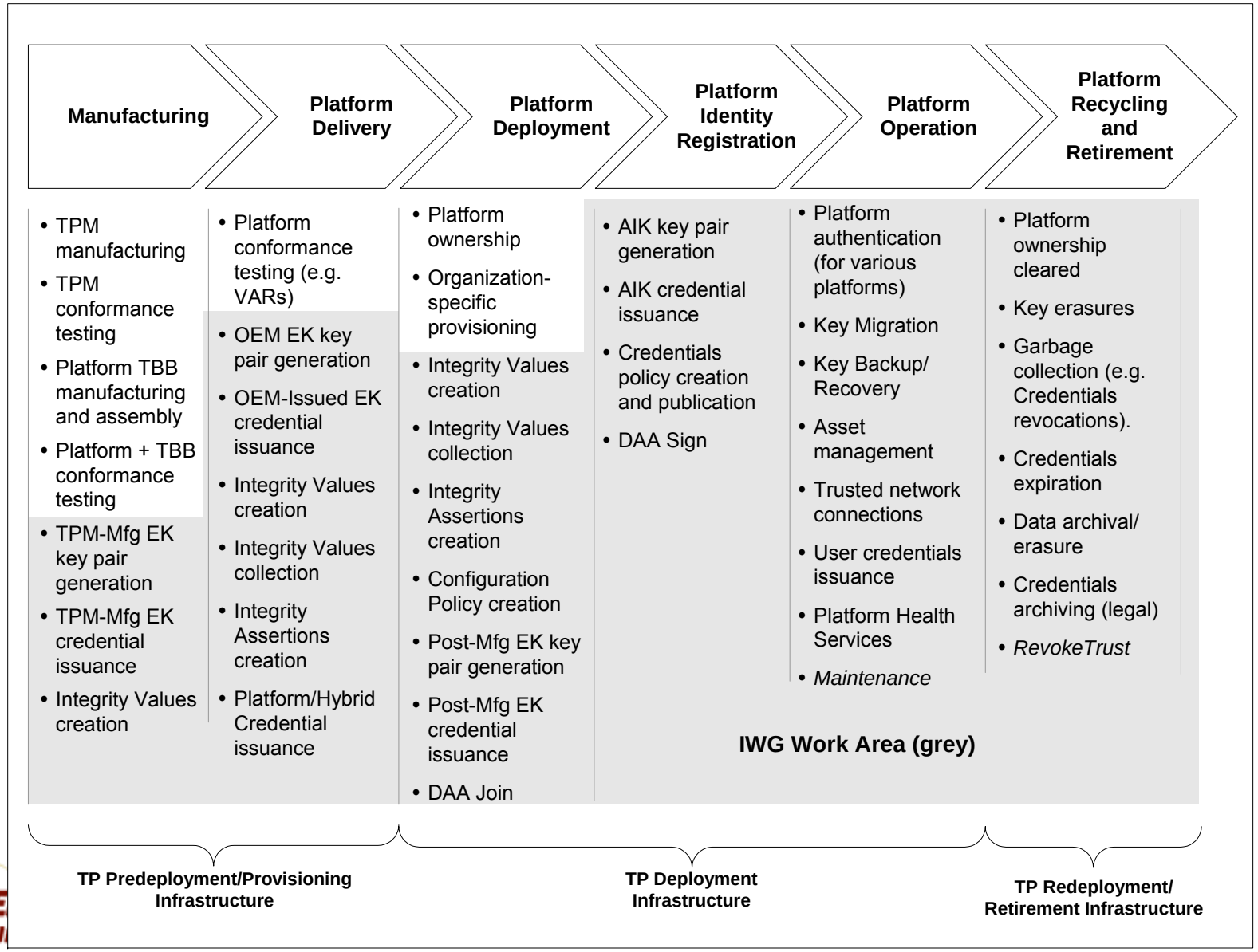
TRUSTED COMPUTING GROUP™

# The Trusted Platform Lifecycle

- The Need for a Lifecycle definition:
  - First step towards understanding how to provide infrastructure for trust establishment
  - All entities in the Supply-Chain identified
  - All their functions defined
  - All their trust-related assertions (which they may issue/imply) are understood/defined
- TP Lifecycle:
  - 6 phases, with 3 broad divisions
    - Provisioning, Deployment, Retirement
  - Multiple functions in a Phase may be done by same entity
    - e.g. OEM also TPM manufacturer
  - One entity may span multiple phases
  - Identical function performed in an earlier phase may result in different trust level when done in a later phase

TRUSTED COMPUTING GROUP™

# The Trusted Platform Lifecycle



# Contents

- The Challenge of Trusted Computing
- The Trusted Platform Lifecycle
- **Model for Infrastructure**
- Model for Platform Authentication
- Use Case: End-Point Integrity
- Summary

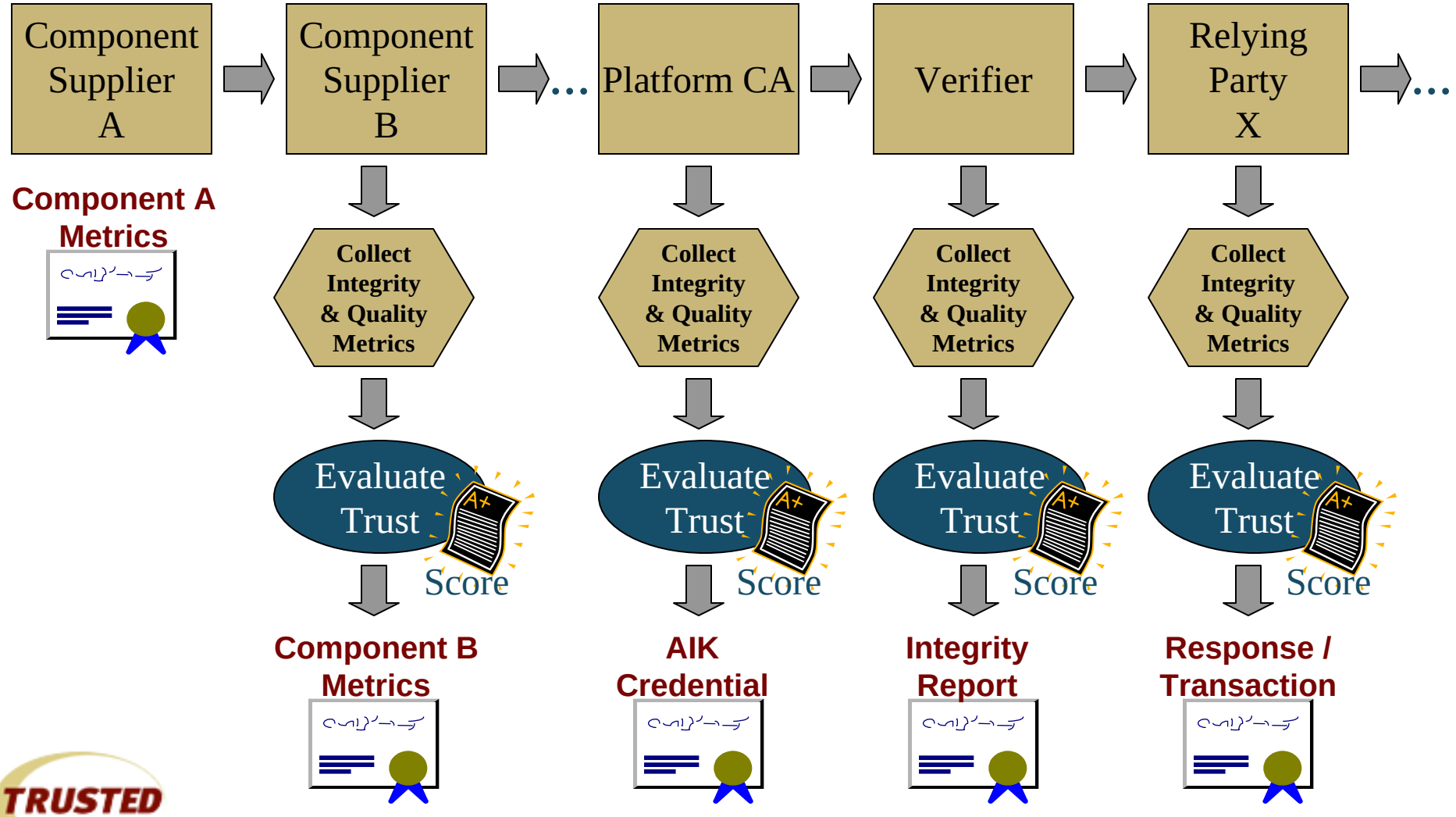
TRUSTED COMPUTING GROUP™

# Model for Trusted Computing Infrastructure

- Objective
  - Infrastructure that bridges manufacturing configuration management process with IT configuration management process
- Requirements
  - Controlled mutability of system components through all stages of the platform lifecycle
- Approach
  - Evaluate quality metrics at the transition points
    - When platform components change hands
    - When making decisions involving risk

TRUSTED COMPUTING GROUP™

# Transition Flow



# Some Observations

- Integrity Metrics are Domain Specific
  - Component Suppliers → Supply Chain
  - Platform CA → Value Added Services
  - Verifier → IT Manageability
    - E.g. Trusted Network Connect & Platform Reporting
  - Relying Party X → Financial etc…
- Participants have things in Common
  - Ability to collect integrity metrics
  - Ability to evaluate trust and score results
  - Ability to control configuration management process
  - Ability to define meaningful components
  - Ability to digitally sign results

Trusted computing relies on interoperable configuration management

TRUSTED COMPUTING GROUP™

# Contents

- The Challenge of Trusted Computing
- The Trusted Platform Lifecycle
- Model for Infrastructure
- **Model for Platform Authentication**
- Use Case: End-Point Integrity
- Summary

TRUSTED COMPUTING GROUP™

# Building Blocks for Trust

- Building Blocks (BB) represent common requirement and behavioral patterns leading to trust establishment
  - Common functions (e.g. authentication, secure storage, etc.)
  - Common components (e.g. credentials, TPM-seal, etc.)
- The TCG IWG has identified over 2 dozen BBs:
  - Set of BBs addresses numerous (over 30) Use-Cases/Scenarios identified by the IWG
  - Platform Authentication BB core to numerous Internet-based transactions
- Platform Authentication BB defined around the IWG 3-party transaction model:
  - Model servers numerous Use-Cases
  - Interpretation open to layer of use (e.g. Apps-layer, Network layer)
  - Informed by the Four Corners model

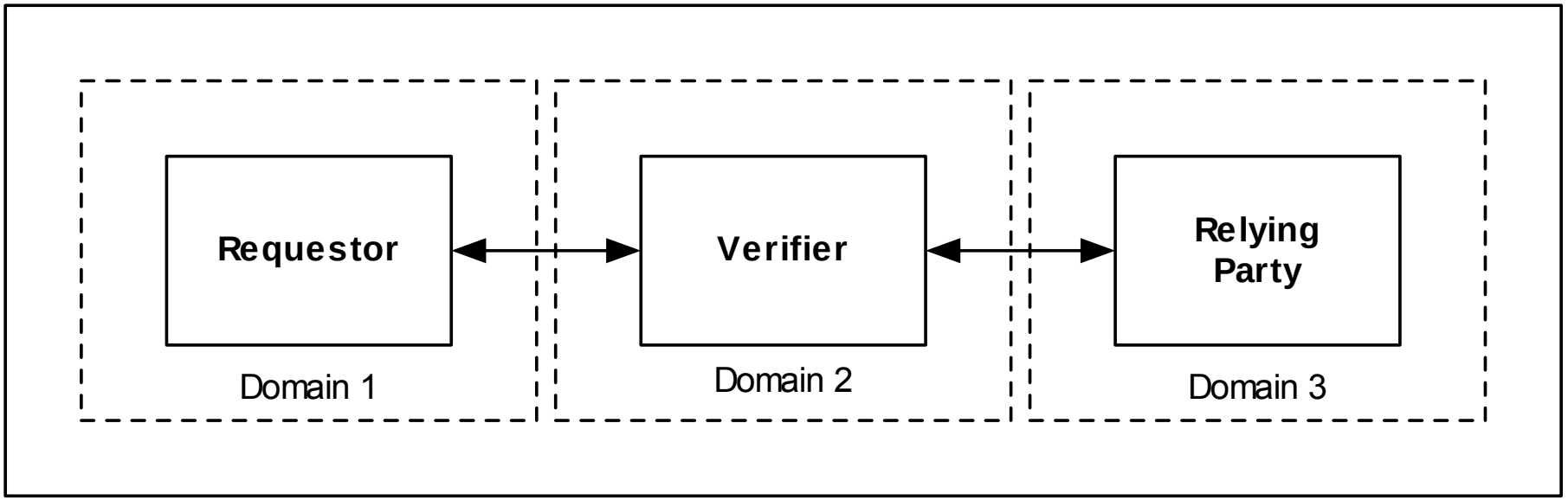
TRUSTED COMPUTING GROUP™

# Model for Platform Authentication

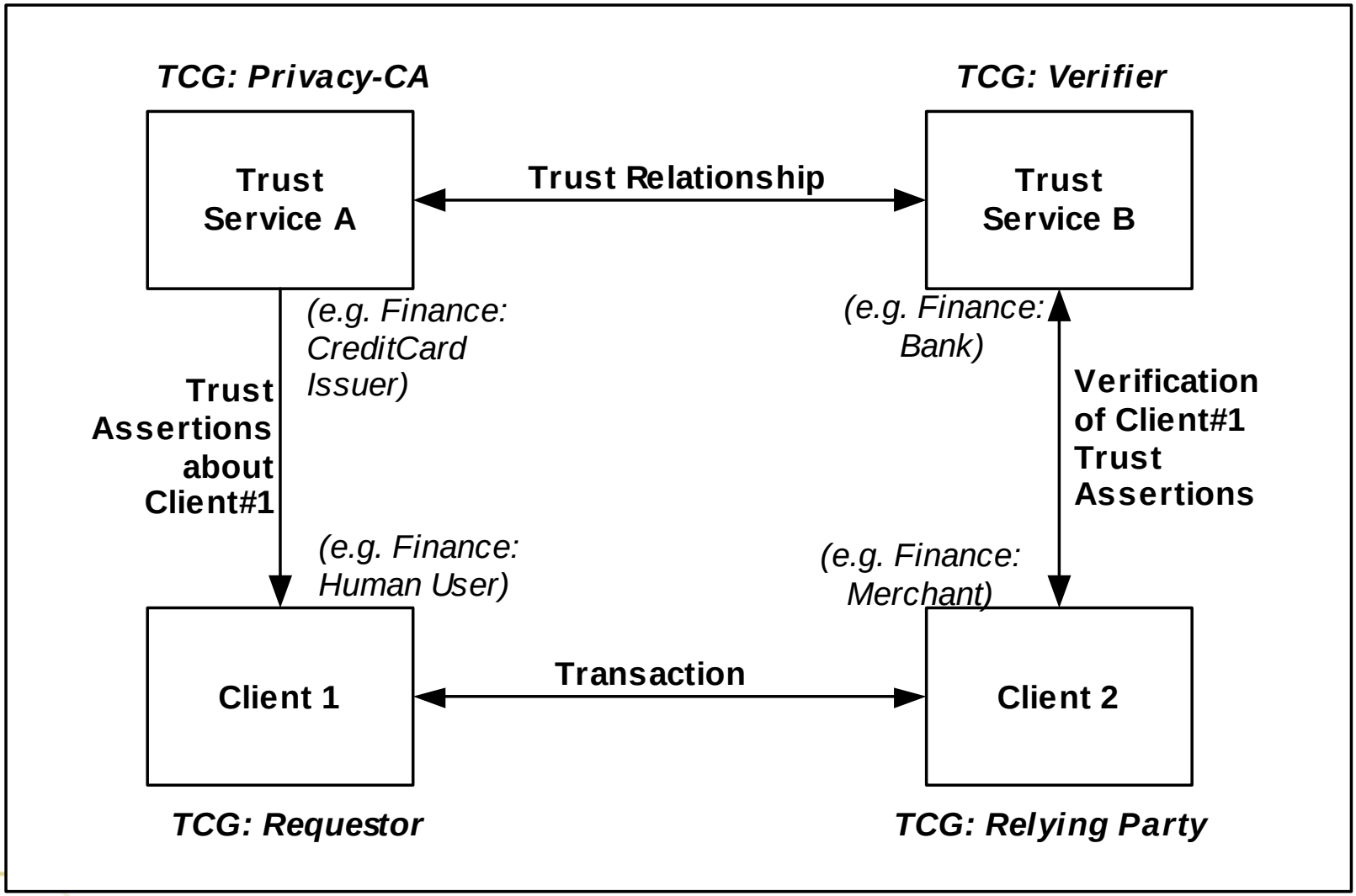
- Conveying TP trust-properties (as part of authentication) is key to TC value-prop
- 3-party model reminiscent of the Four-Corners Model
  - *Requestor* seeks services or access to resource from the *Relying-Party*
    - Relying-Party can either evaluate itself or rely on a *Verifier* to evaluate trust properties and assertions of Requestor
  - *Verifier* performs the evaluation of the Requestor's assertions
  - Outcome of the Verifier's evaluation can be binary or a trust score

TRUSTED COMPUTING GROUP™

# Basic Model for Platform Authentication

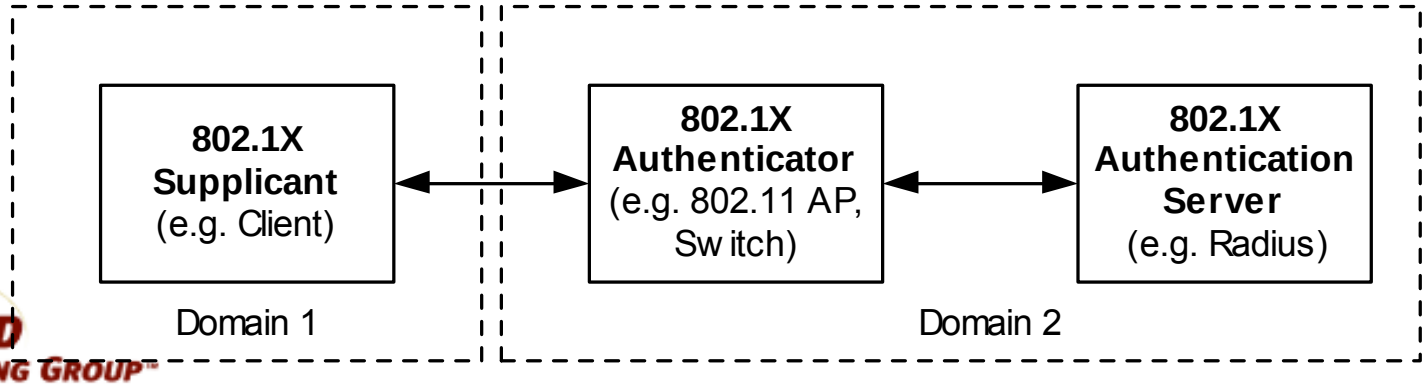


# Four Corners Model: A Precedent

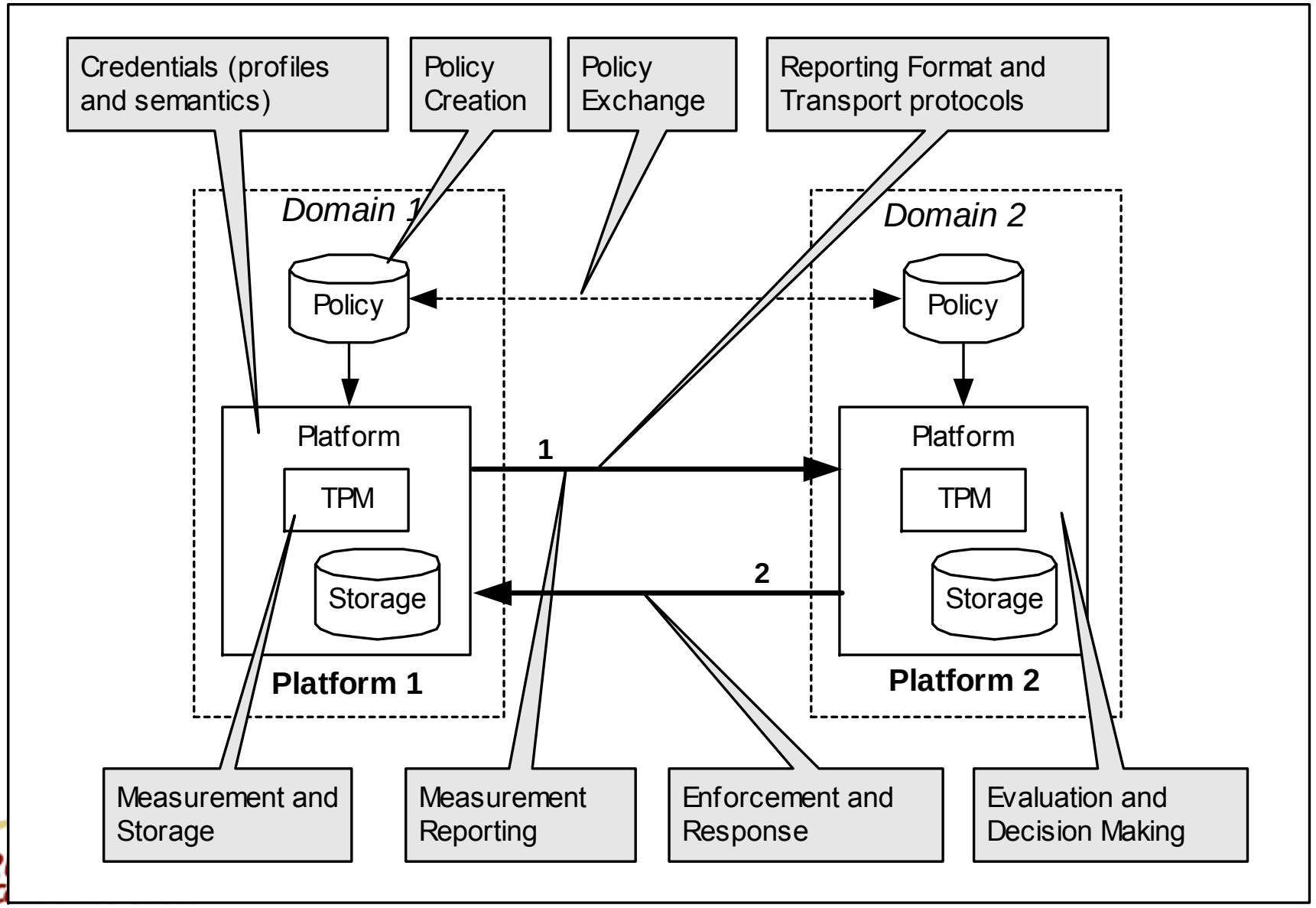


# Model Applicability

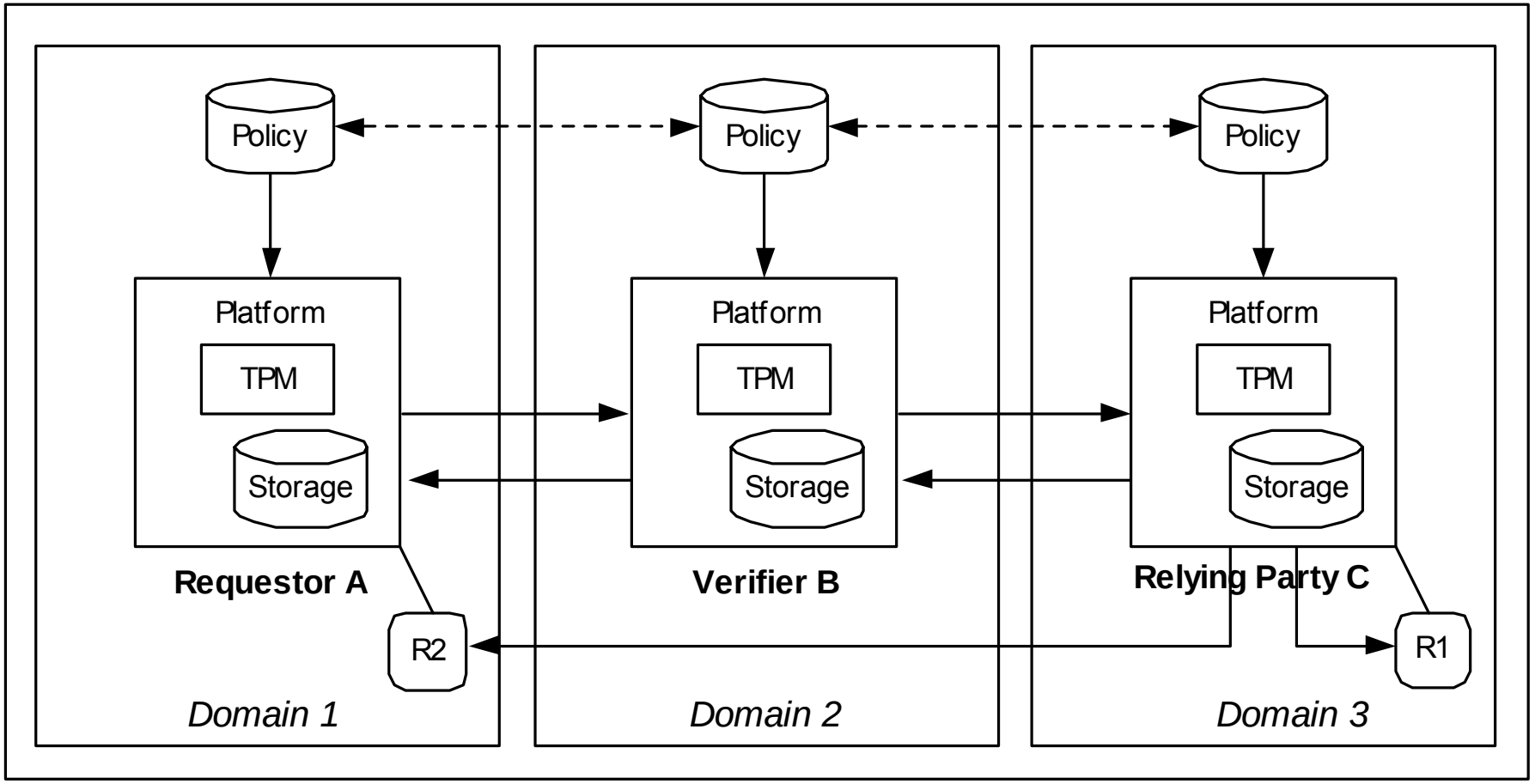
- The model applies at different layers and useful for broad set of scenarios
- Example: Network authentication
  - "Machine-to-machine" authentication
  - Basis for end-point authentication and end-point integrity evaluation
  - Network layer authentication
    - e.g. 802.1X, VPNs, etc



# Components of Authentication Model



# Platform Authentication Model



# Contents

- The Challenge of Trusted Computing
- The Trusted Platform Lifecycle
- Model for Infrastructure
- Model for Platform Authentication
- **Use Case: End-Point Integrity**
- Summary

TRUSTED COMPUTING GROUP™

# Use Case: End-Point Integrity

- End-Point Integrity a growing area of interest to Networking Industry:
  - Notion of “health” of a client computer wishing to gain Enterprise-network access
    - Health = AV-version, OS Patch, drivers, etc.
  - Authentication Server evaluates health level of the client
  - Healthy clients allowed network access, unhealthy clients denied or placed into remedial network
- Current industry efforts:
  - Microsoft’s *Network Access Protection* (NAP)
  - Cisco’s *Network Admission Control* (NAC)
  - TCG’s *Trusted Network Connect* (TNC)

TRUSTED COMPUTING GROUP™

# Summary

- Trusted Computing (TC) as a new paradigm in computing
- The TPM is the starting point – but an entire new infrastructure is needed to support TC
- TP Lifecycle – identifying phases and function in a TP's life
- Platform authentication as core building block for TC
- Numerous Use Cases – End-Point Integrity most appropriately addressed using TC technologies