Trust and security in dynamically aggregated web services

Paul Kearney
Security Research Centre, BT
CASSIS Workshop, Nice, March 2005

Introduction

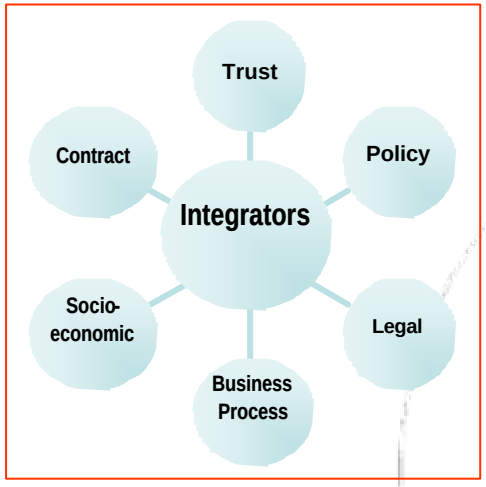
- The classic web service vision anticipates a large number of disparate services being offered over the Internet by different individuals and companies.
- In response to a requirement from an end-user a process of discovery, selection and negotiation will result in the assembly of a composite service well-matched to the requirements of that user, at that time, performing that activity in that location.
- The resulting composite service is provide by a Virtual Organisation (VO) of autonomous commercial entities with different trust relationships and security policies
- The current ‘Standard Model’ of web services trust and security is not sufficient to provide for ad hoc VOs.
- Argue that establishing a clear semantics is a necessary pre-requisite for progress.

Outline of talk

- Introduction to the TrustCoM project
- The emerging ‘Standard Model’ for web services security
- A conceptual model based on speech act semantics
  - Or at least the beginnings of one
  - Associates declarative semantics with ‘Standard Model’ constructs
  - Introduces a computational notion of Trust along the way

Introduction to the TrustCoM project
http://www.eu-trustcom.com

TrustCoM Consortium



Technical Experts
Sector-specific expertise
Drive research innovation

Integrators
Broad knowledge of both technological and research state of the art
Capable of blending together research innovation and materialising it into innovative ICT solutions

Advisors
Scientific experts and potential user groups
Offer consultancy and monitor project progress

TrustCoM Project Objectives

R&D type

To provide a **trust & contract management framework** enabling the definition and secure enactment of

R&D focus

collaborative business processes within secure, scalable, highly dynamic, integrated and targeted **Virtual Organisations,**

R&D relevance

which are **formed on-demand**, are **self-managed** and **evolve dynamically**,

Technology focus

sharing computation, data, information and knowledge **across enterprise boundaries**,

Business need

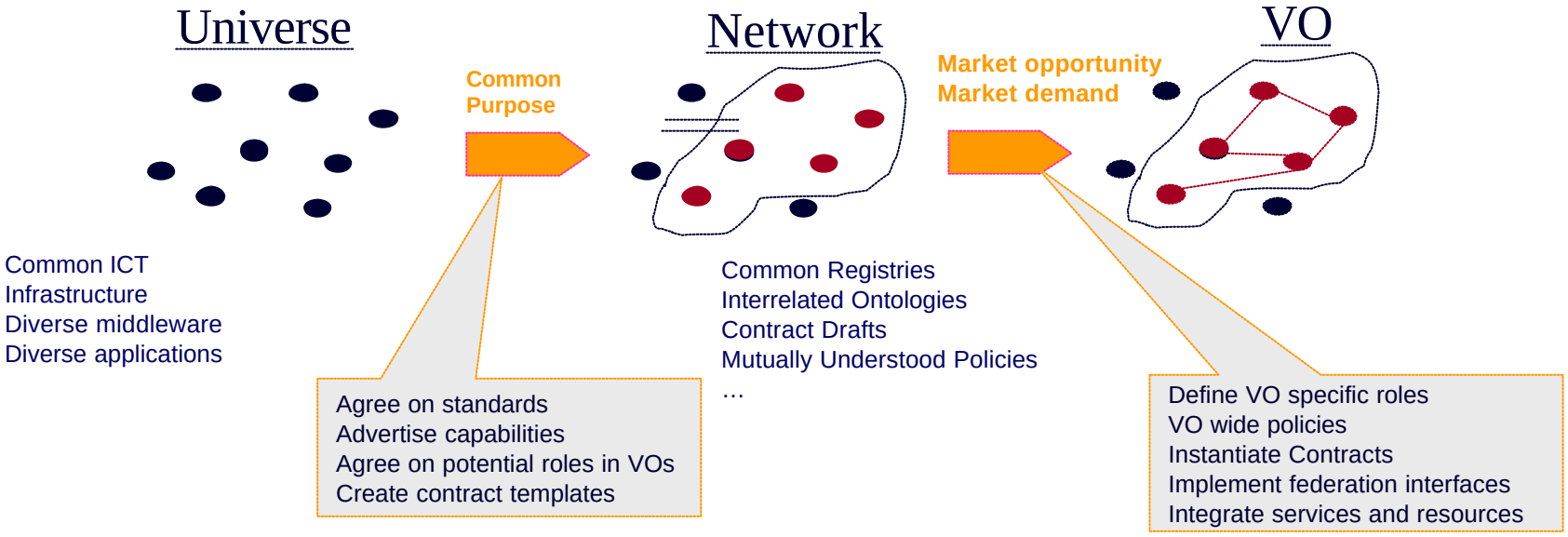
in order to

- tackle collaborative projects that their participants could not undertake individually or
- collectively offer services to customers that could not be provided by the individual enterprises.

What is a Virtual Organisation?

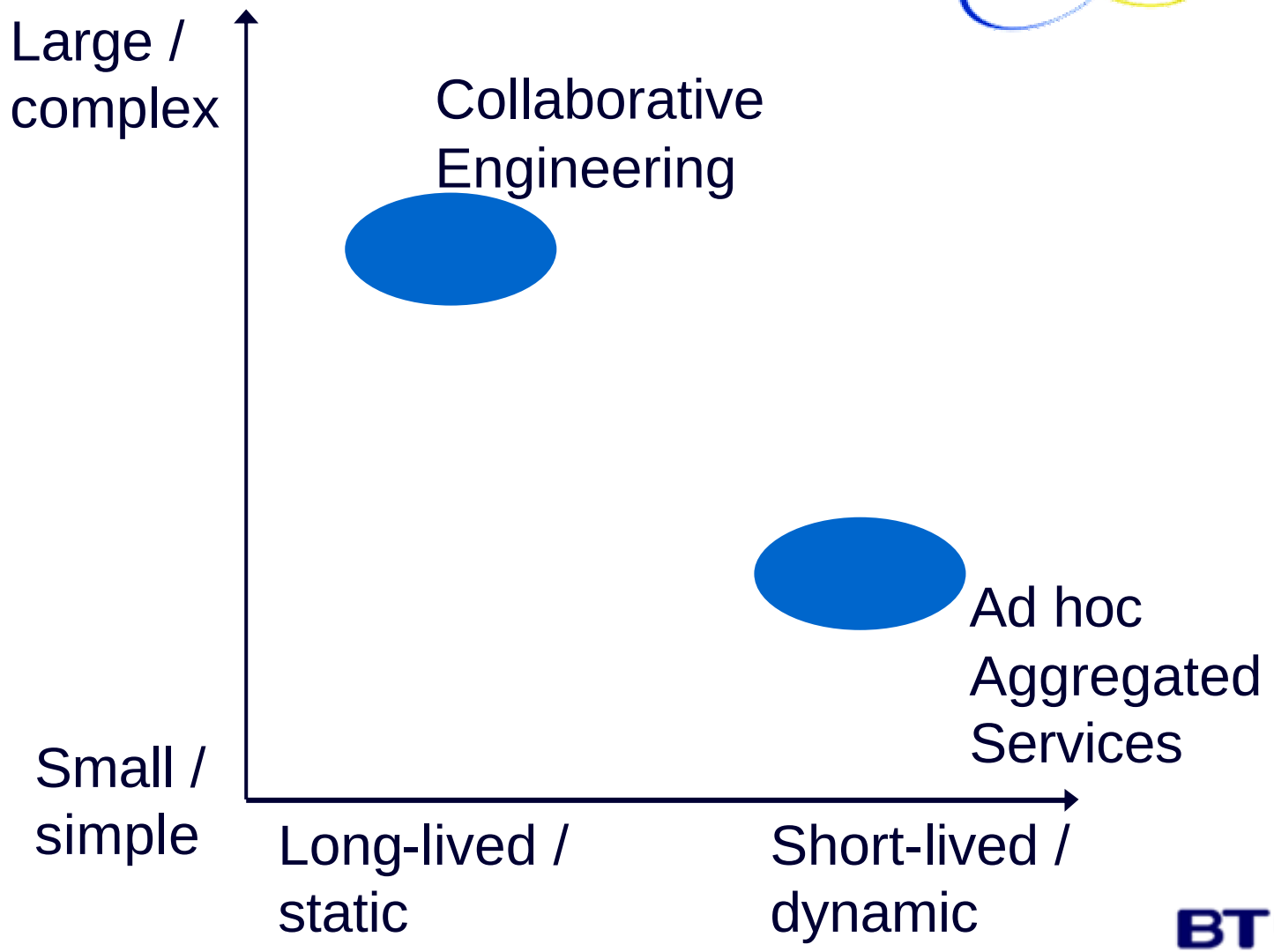
A temporary or permanent coalition of geographically dispersed individuals, groups, organisational units or entire organisations that pool resources, capabilities and information to achieve common objectives.

- can provide services and thus participate as a single entity in the formation of further VOs.
- enables creation of recursive structures with multiple layers of "virtual" value-added service providers.



The parties that form a virtual organization are typically part of a larger enterprise network of which a selection of partners is made. Participation in the network indicates disposition to work together in a future market opportunity.

VO space


Large / complex
Collaborative Engineering
Ad hoc Aggregated Services
Small / simple
Long-lived / static
Short-lived / dynamic

The emerging ‘standard model’ for web services security

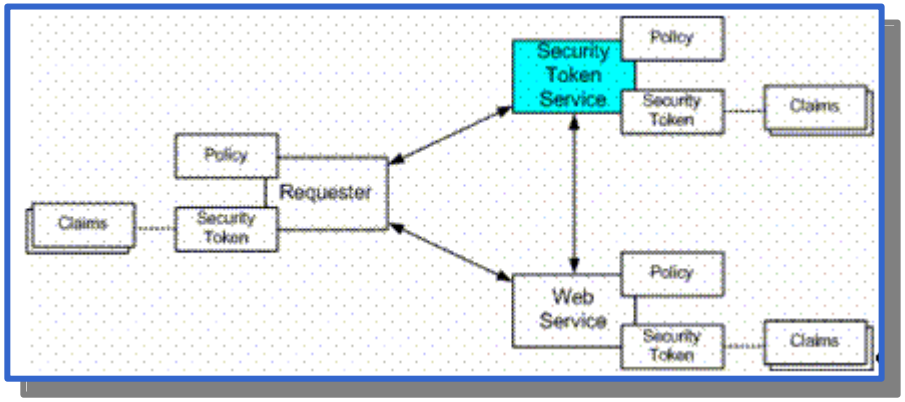
State of the art in web service security

- Except in simple situations, it is difficult to provide end-end security via transport layer mechanisms (HTTPS / SSL) alone. Need message level security.
- Growing consensus on conceptual building blocks for message level security.
- 'Foundation' specifications firming up (XML Encryption, XML Signature, WS-Security, SAML, ...), but still fluid, vendor implementation patchy and interoperability doubtful. Further layers of specification need to be added.
- You can implement message level security, but need to establish local conventions. Vision of carefree, open interoperability still some way off. (Not just due to security).

The emerging WS-* security model

Introduces security contexts and security context tokens

Deals with issues of crossing 'trust domains' -- pretty vague



Language for asserting requirements on msg features
- confidentiality
- integrity
- token
- visibility
- header
- age

WS-SecureConversation	WS-Federation	WS-Authorization
WS-Policy	WS-Trust	
WS-Security		
SOAP Foundation		

To do with requesting, issuing and checking tokens

•XML encryption (msgconfidentiality)
•XML DSIG (msg integrity)
•Tokens: claims

From MS/IBM WS security roadmap

… and the other lot: Liberty + SAML

- Project Liberty / Liberty Alliance
  - Federated identity management
- Security Assertion Mark-up Language (SAML)
  - OASIS standard
  - XML-based language for making ‘assertions’ about security
- Assertion
  - a statement made by an ‘authority’
  - can be signed to identify authority reliably
  - if you trust the authority, you tend to trust the truth of the statement
  - can be time-stamped, etc., to establish bounds to validity
- Defines three types of assertion
  - Authentication
  - Authorisation
  - Attribute

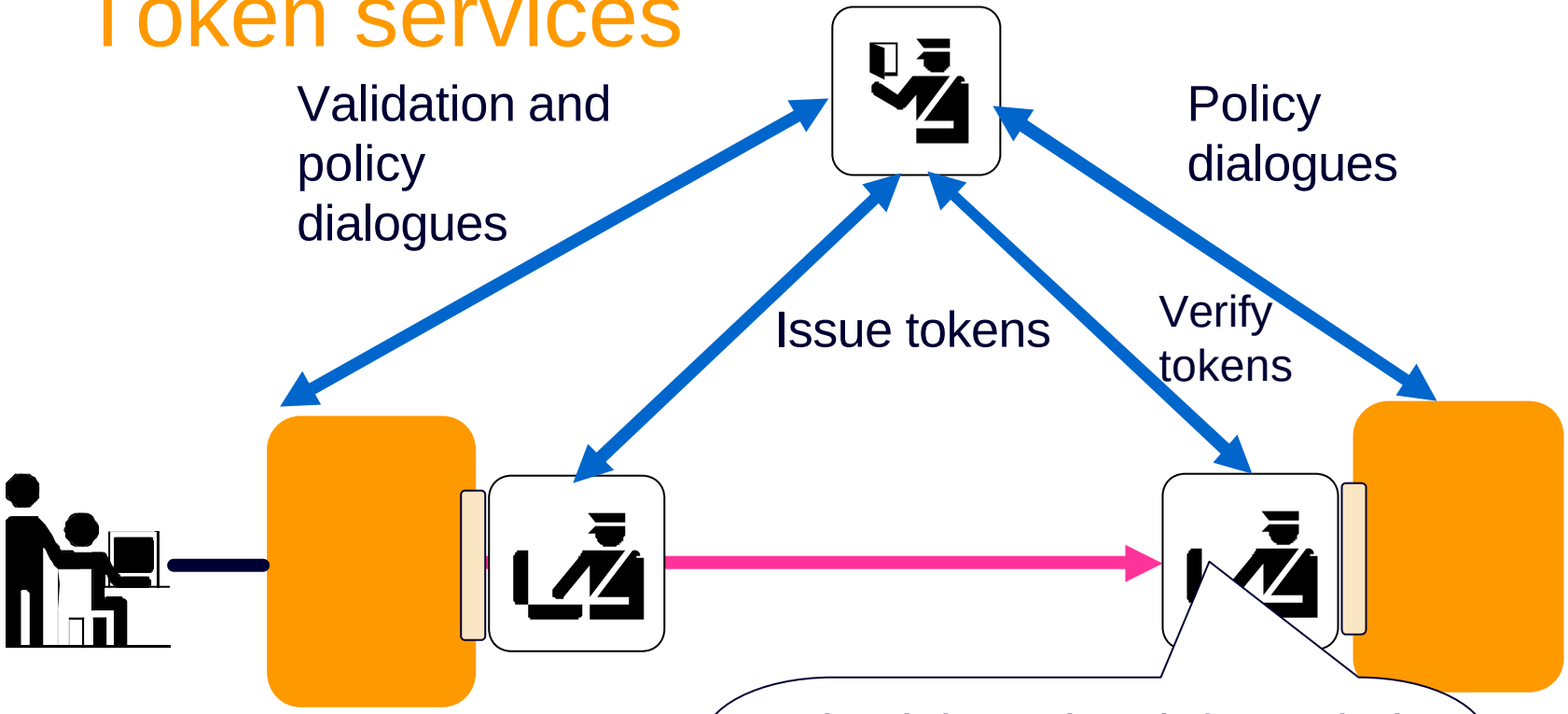
and correspond query and response messages

- Authentication assertion:
  - states what checks have been done to authenticate an identity claim
- So, there seems to be a fair consensus on the basic model

Web Services Security building blocks

- public key cryptography and digital certificates
- digital signatures used to bind elements of the message and assure integrity
- encryption of messages for message confidentiality (where required)
- use of security software tokens carried in message header to communicate ‘claims’
- use of trusted identity / token services to issue tokens
- policy-based access control

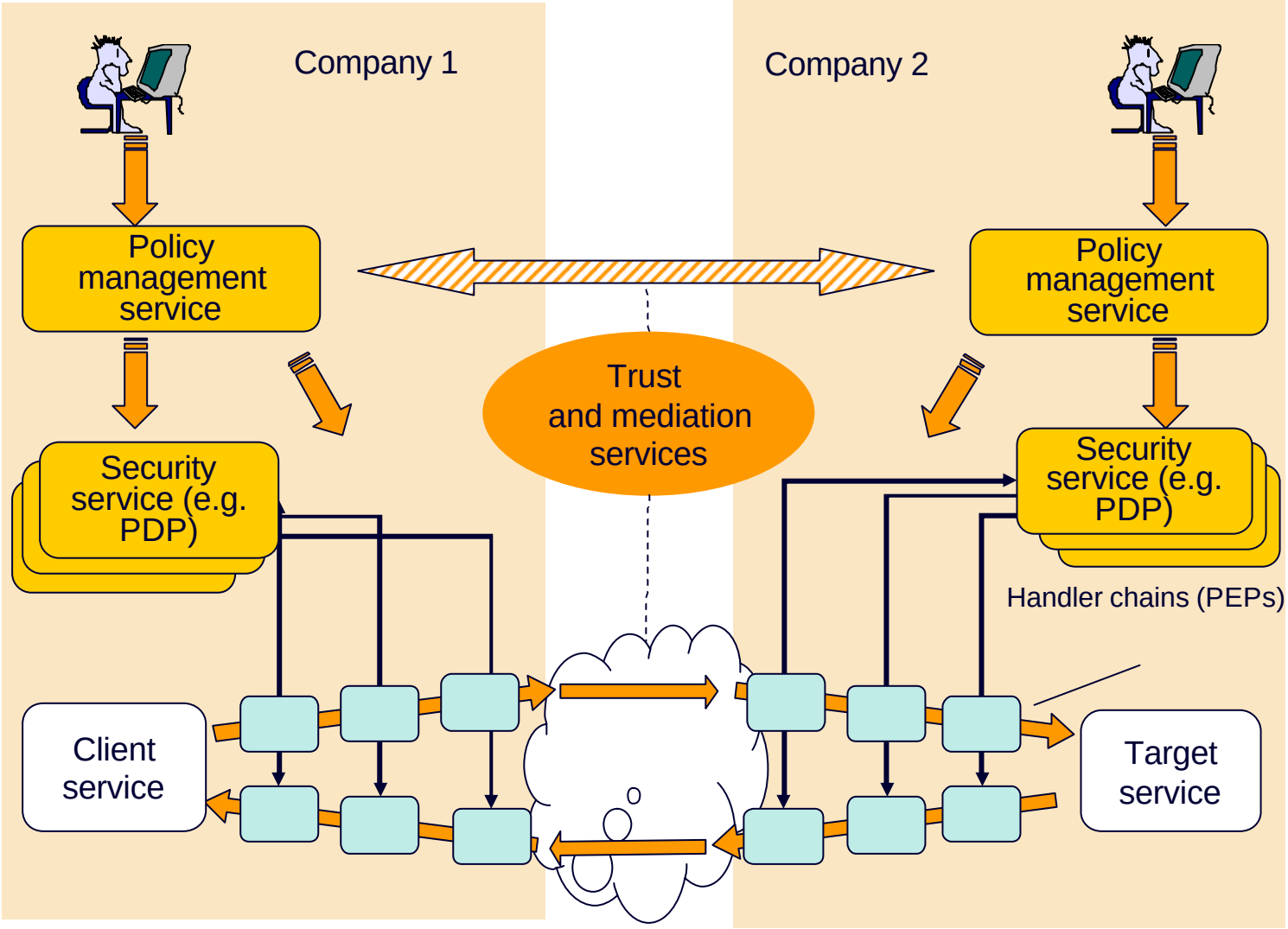
Token services



Check based on info carried with the message (tokens)

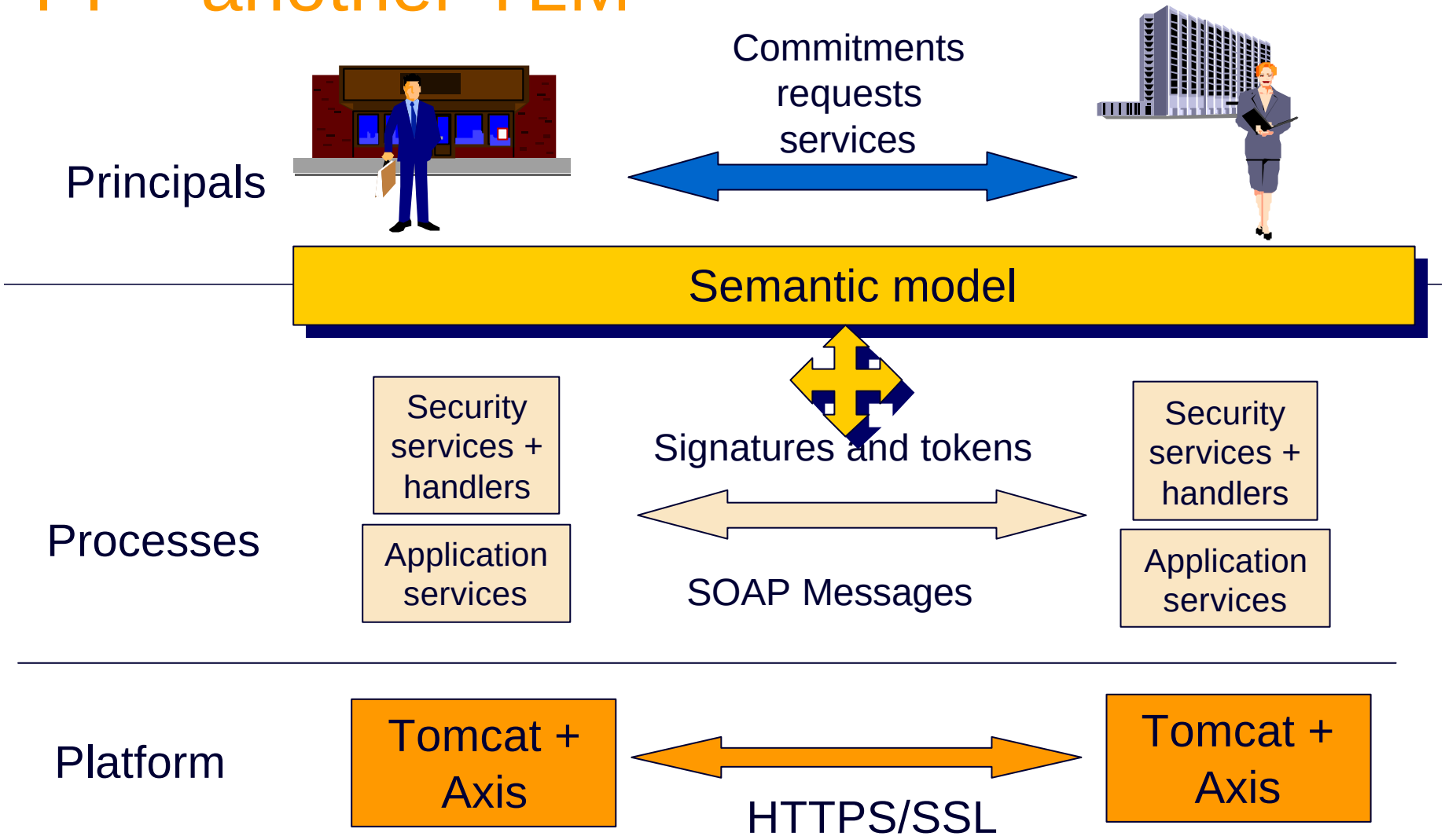
- direct evidence
- explicit assertion by authority
- implicit assertion by authority (e.g. ticket)

Security architecture



Web service semantics

PPP - another TLM



Web service semantics

- View a WS as providing managed access to a resource
- Simple transaction types:
  - request that an operation is performed on a resource (and return result)
  - request information about service (or resource?)
  - Notification
  - Can build more complex transaction types from these
- WS has an owner (e.g. an enterprise)
- Resource also has owner
  - Delegates responsibility to WS
- WS acts on behalf of a ‘legal entity’ (user, enterprise, etc.)
  - can have ‘pure client’ WSs that only represent their agent in interactions with other WS (I.e. no associated resource)
- WS runs on a platform / host

Resources and operations

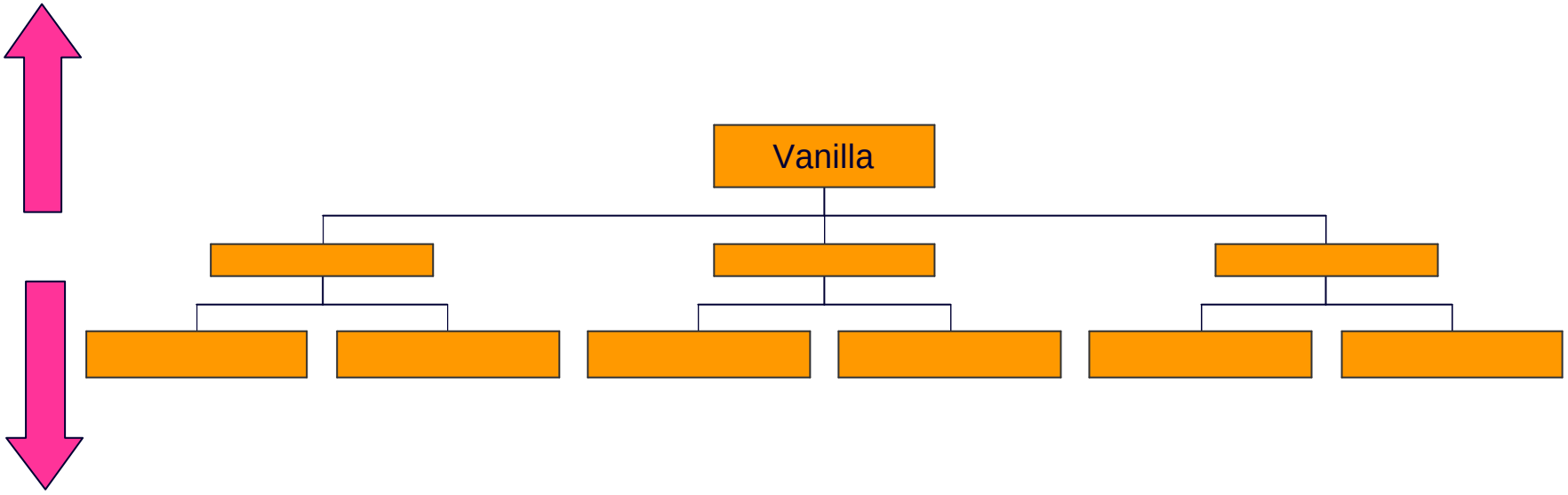
- Object-oriented viewpoint
  - resources as objects, operations as methods
  - methods (operations) are specific to classes (resource types), but …
  - try to maintain semantic consistency
    - methods with the same name should do analogous things
  - use inheritance (specialisation) hierarchy
    - abstract semantics specialised to inheriting classes

Common resource abstractions

- Document
  - Descriptor
    - Identity
  - Template
- Reference (‘pointer’)
- Collection
  - Repository (Collection of Documents)
  - Grouping (Collection of References)
- Operations common to all Collections:
  - add, delete, find
  - & composites:
    - replace: delete + add but keep same reference
    - modify: find + apply operation to retrieved item

Service ontology / class hierarchy

More abstract / general



More concrete / specific

Message semantics

Speech acts (very simplified)

- Elements of message
  - Basic statement
  - Speech act category applies inflection to statement
  - Sender and Receiver
  - Plus: ontology, conversational context, etc.
- Message = statement about the sender's mental state made with the intention of influencing receiver's behaviour
- Mental state:
  - beliefs, desires, intentions (BDI)
  - beliefs, commitments (Shoham's AOP)
- **Inform**: I believe X to be true
- **Agree/commit**: I intend / promise /to do X
- **Request:**
  - (action) I would like X to happen / Will you do X?
  - (information) I would like to know X / Please tell me X.

Speech act interpretation of WS message

- Message body = speech act + basic statement
  - RPC encoding relatively straightforward (but limited)
    - “request” +action + parameters (**request**)
    - “response” + action + result (**inform**)
    - Still need ontology/typology for resources and actions (next slide)
  - Document encoding
    - Need to establish a semantic framework such that document types (information model) have semantic interpretation
    - Scope for richer semantic model encompassing business transations and processes
      - cf ebXML, RosettaNet, TMF, etc.

‘Header’ semantics - Sender & receiver

- WS-Addressing provides syntactic hooks, but need to be extended
- Make distinction between WS and legal entity it represents
- Need to able e.g. to identify sender as:
  - WS1 acting on behalf of legal entity Fred Bloggs of ABC Inc.

  Or even
  - WS2 acting for WS1 acting for legal entity Fred Bloggs of ABC Inc.
- Relationship between employee / representative, role and enterprise.
- Once we establish relationships among Message, Action, Resource, Sending and Receiving WSs and Principals, can write meaningful RBAC policies.

‘Header’ semantics – Signatures and encryption

- Encryption – semantics not required
- Signatures
  - Dangerous to associate semantics with signature unless explicit within context (e.g. of document type / element)
  - Safest just to regard as evidence that signed elements have not been altered since leaving the ‘signer’
    - Preferable to endorse with time and ‘place’ on message path
- But note ambiguity:
  - Certificates issued to legal entities (with semantic context), but
  - Keys held and used by computational entities (WS or host)
- Need to be sure that computational entity can act for certificate owner in this context
  - Preferable to make association explicit

‘Header’ semantics – Tokens

- Message headers provide a ‘control’ communication channel among SOAP nodes on message path
- Security enforcement points communicate via tokens
- Types of security token
  - Proof of identity / rights by possession
    - Proof of possession by presentation
    - Proof of knowledge without revelation of secret
  - Assertion by trusted authority, e.g.
    - Certificate
    - SAML assertion
- ‘Inform’ speech act semantics can be associated with assertions
  - Probably give implicit interpretation to ‘proof of possession’ tokens too.

Trust and speech acts

- Trust is confidence in the correct behaviour of another when in a situation of dependence
  - I can be said to trust you if
    - I have no control over whether you behave correctly, and
    - I willingly put myself in a situation where I will lose out if you do not behave correctly
- If I trust you (in a given context)
  - I will tend to believe the information you tell me
  - I will tend to believe you will fulfil your commitments
- Trust of agent A in agent B is the tendency for A to believe and act upon speech acts uttered by B in a given context
  - Direct vs. reported
  - Dimensions: truthfulness, competence, benevolence, …

Authorities and assertions

- Assertion
  - a statement made by an ‘authority’
  - can be signed to identify authority reliably
  - can be time-stamped, etc., to establish bounds to validity
- SAML defines three types of assertion
  - Authentication (states what checks have been done to authenticate an identity claim)
  - Authorisation
  - Attribute

  and correspond query and response messages
- Authority is just an agent with some credibility on the topic
  - if you trust the authority, you tend to trust the truth of the statement

The new (XML-based) protocol stack

Collaboration level

Conversation level

Transaction level

Basic message pattern level:

one-way, synchronous request-response, asynchronous request-response

---

Message level:

SOAP + extensions

Transport / connection:

HTTP, FTP, MQ Series, ...

⋮

Summary

- Have described basis of a reasonable declarative semantics for SOAP messages and security assertions based on speech acts
- Semantic model also needs to include business documents (message body), processes and relationships
  - Number of alternative ‘standards’ is a worry
  - Need a more systematic approach to XML-based business languages
- Current message standards lack
  - Richer set of roles associated with a message (not just sender and receiver)
  - Means of associating identity claims in header with roles in message and body content
- Within TrustCoM exploring:
  - Federated ‘knowledge enabled’ VO infrastructure
  - Trust and security services that make use of it
  - Dynamic federation of trust services to support ad hoc VO

Questions?