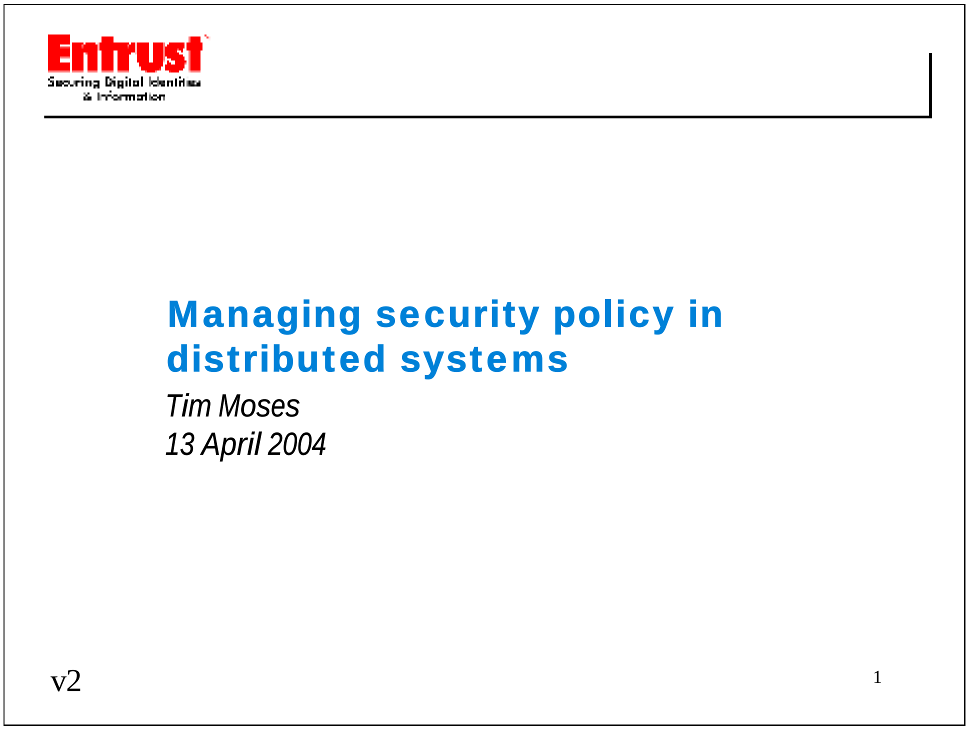


Entrust

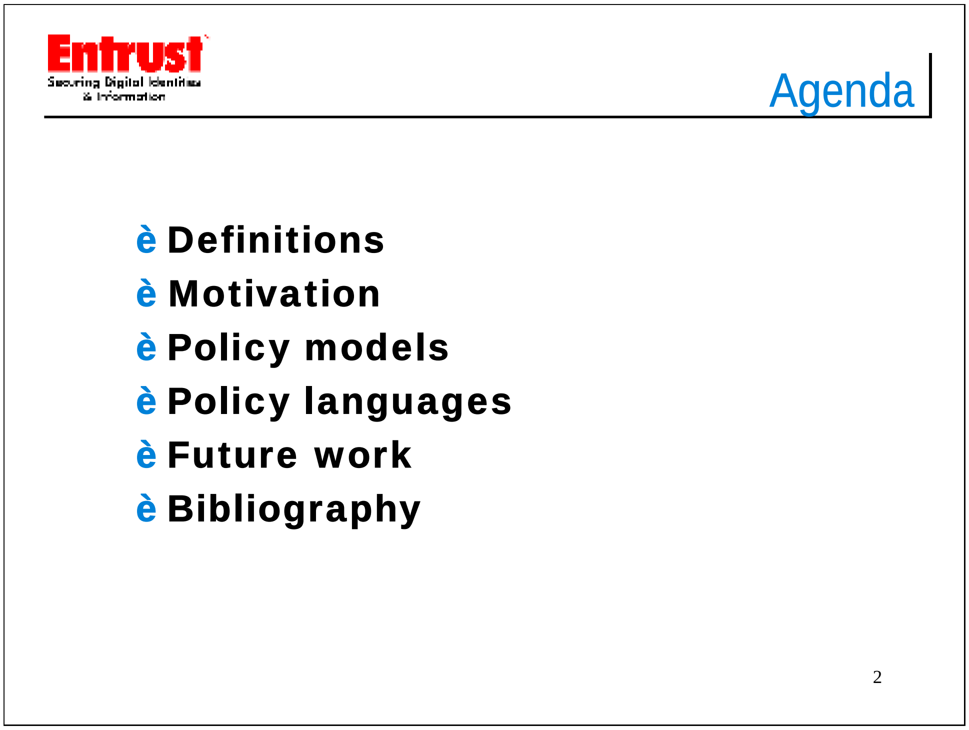
Securing Digital Identities & Information

Managing security policy in distributed systems

Tim Moses

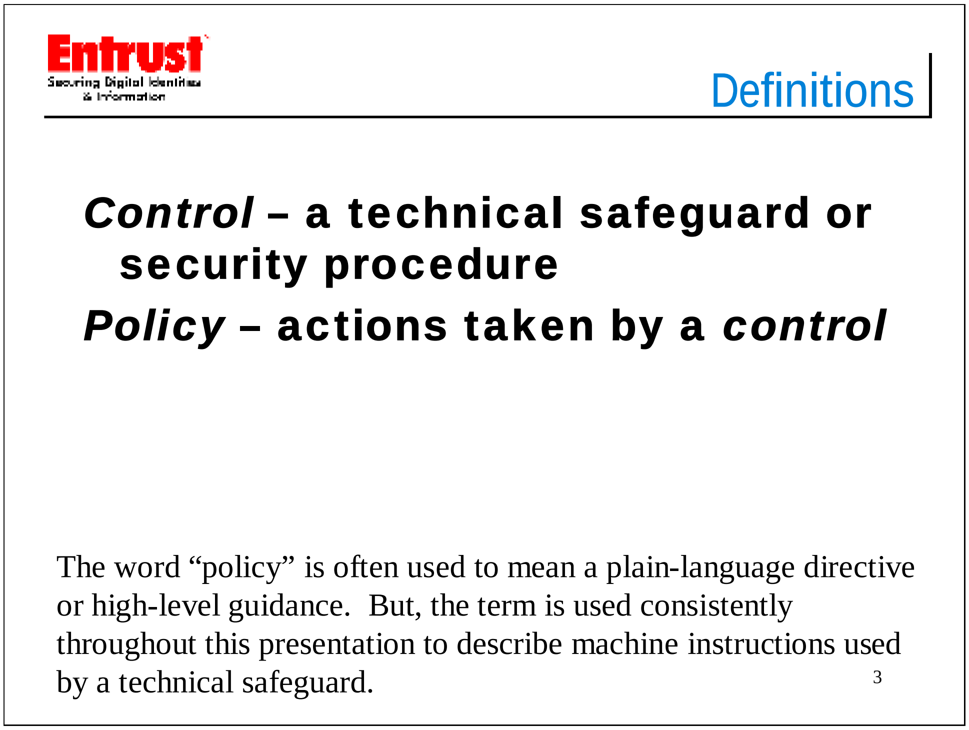
13 April 2004

v2



Agenda

- Definitions
- Motivation
- Policy models
- Policy languages
- Future work
- Bibliography



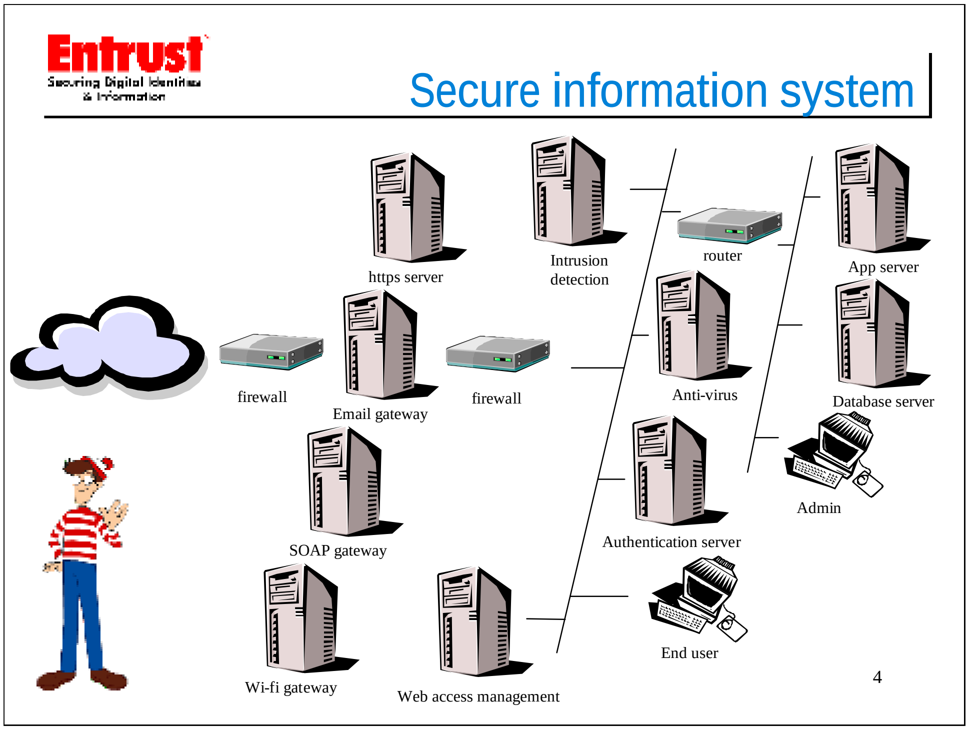
Entrust
Securing Digital Identities & Information

Definitions

Control **– a technical safeguard or security procedure**

Policy **– actions taken by a** ***control***

The word "policy" is often used to mean a plain-language directive or high-level guidance. But, the term is used consistently throughout this presentation to describe machine instructions used by a technical safeguard.

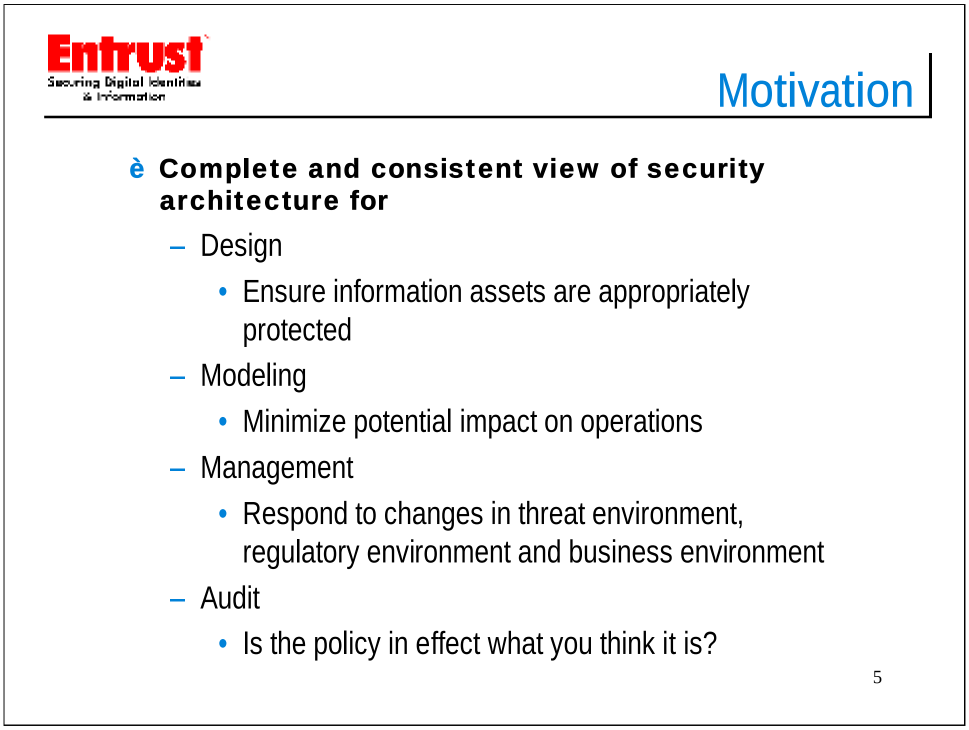


Secure information system

How many controls can you spot in this picture?

All the controls are configurable by policy definition, using separate consoles.

Difficult to get an overall view of security, either by design or actually in effect in the system.



Motivation

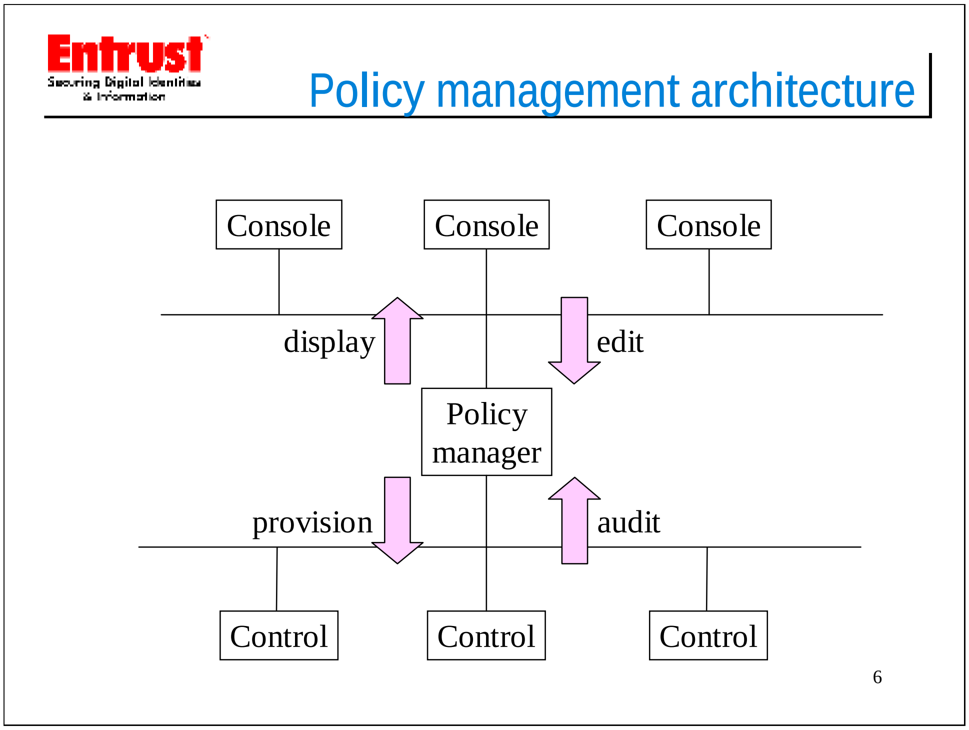
- **Complete and consistent view of security architecture for**
  - Design
    - Ensure information assets are appropriately protected
  - Modeling
    - Minimize potential impact on operations
  - Management
    - Respond to changes in threat environment, regulatory environment and business environment
  - Audit
    - Is the policy in effect what you think it is?

5

Design – cost of controls commensurate with the risk (expected rate of loss)

Regulations and generally-accepted information-security practices.

Modeling – what-if analysis.



Entrust
Securing Digital Identities & Information

Policy management architecture

6

Distributed authorship.

Workflow approval.

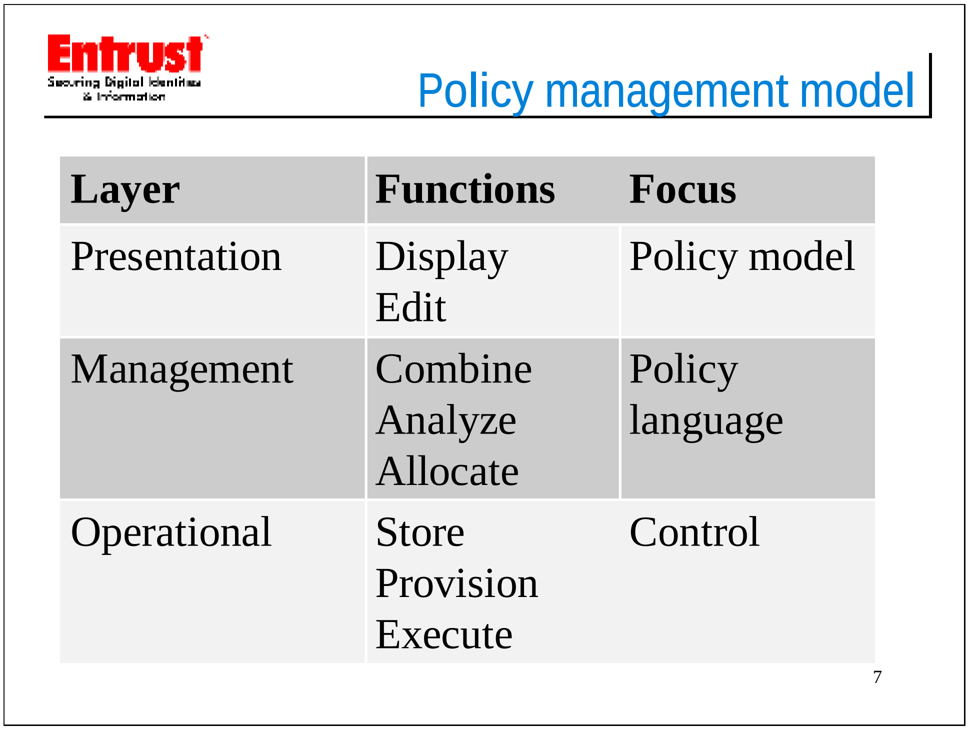
Central repository.

Heterogeneous controls.

Real-time update.

Closed-loop.

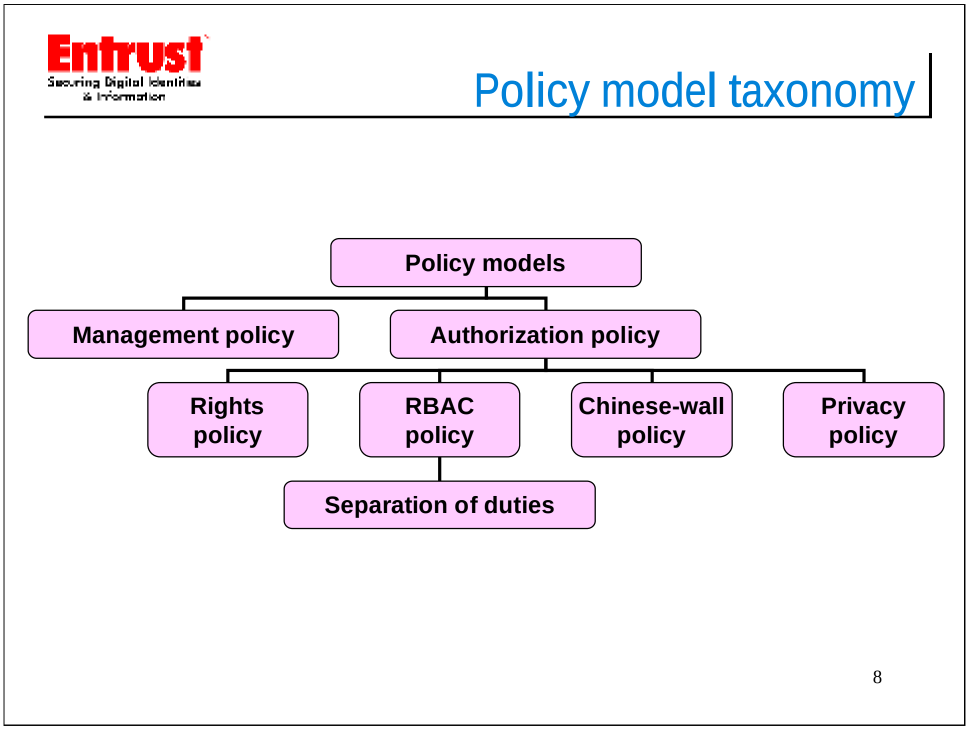
Be careful – avoid single-point of failure.



Entrust
Securing Digital Identities & Information

Policy management model

Layer	Functions	Focus
Presentation	Display Edit	Policy model
Management	Combine Analyze Allocate	Policy language
Operational	Store Provision Execute	Control



Policy model taxonomy

Policy models

Management policy

Authorization policy

Rights policy

RBAC policy

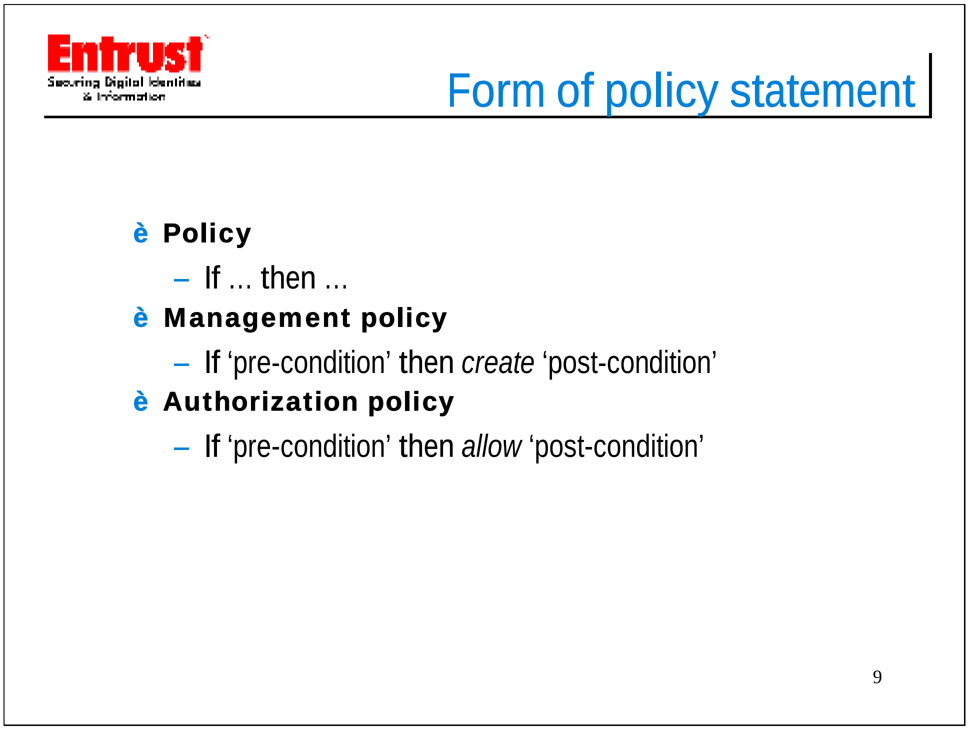
Chinese-wall policy

Privacy policy

Separation of duties

8

The authorization policy taxonomy is incomplete. Cryptographic security policy and trust policy are two other types of policy.



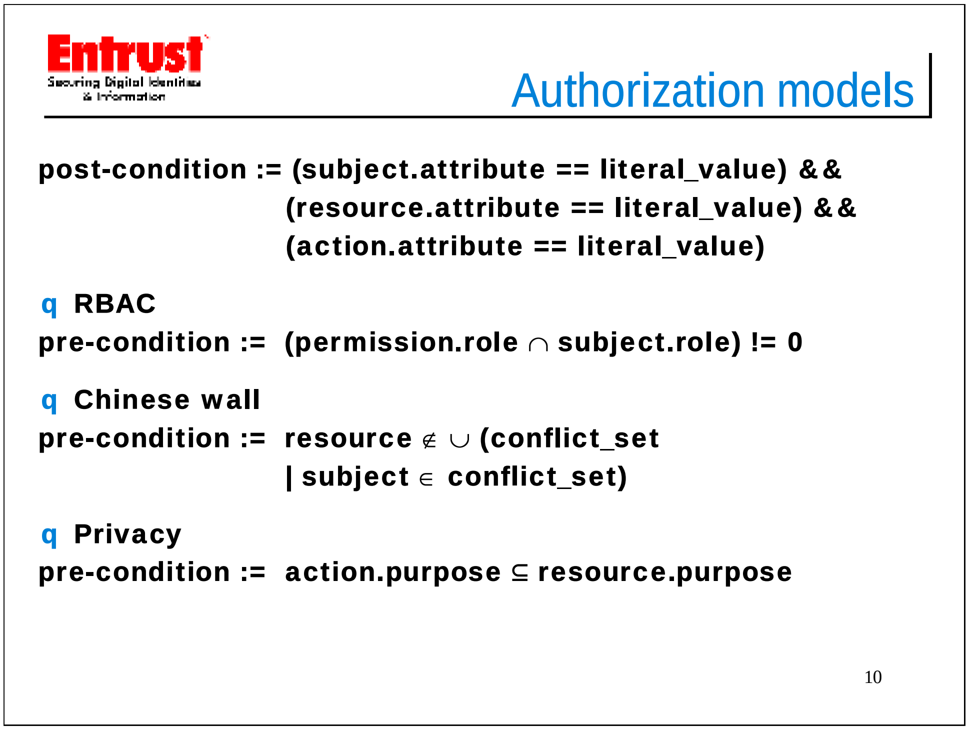
Form of policy statement

- **Policy**
  - If … then …
- **Management policy**
  - If ‘pre-condition’ then *create* ‘post-condition’
- **Authorization policy**
  - If ‘pre-condition’ then *allow* ‘post-condition’

Management policy pre-condition and authorization policy pre-condition and post-condition are predicates, i.e. statements whose truth can be evaluated.

Management policy post-condition is a set of instructions.

Authorization policy pre-condition may be null, then the specified post-condition is allowed to occur unconditionally.



Entrust
Securing Digital Identities & Information

Authorization models

post-condition := (subject.attribute == literal_value) &&
(resource.attribute == literal_value) &&
(action.attribute == literal_value)

q **RBAC**
pre-condition := (permission.role $\cap$ subject.role) != 0

q **Chinese wall**
pre-condition := resource $\notin$ $\cup$ (conflict_set
| subject $\in$ conflict_set)

q **Privacy**
pre-condition := action.purpose $\subseteq$ resource.purpose

10

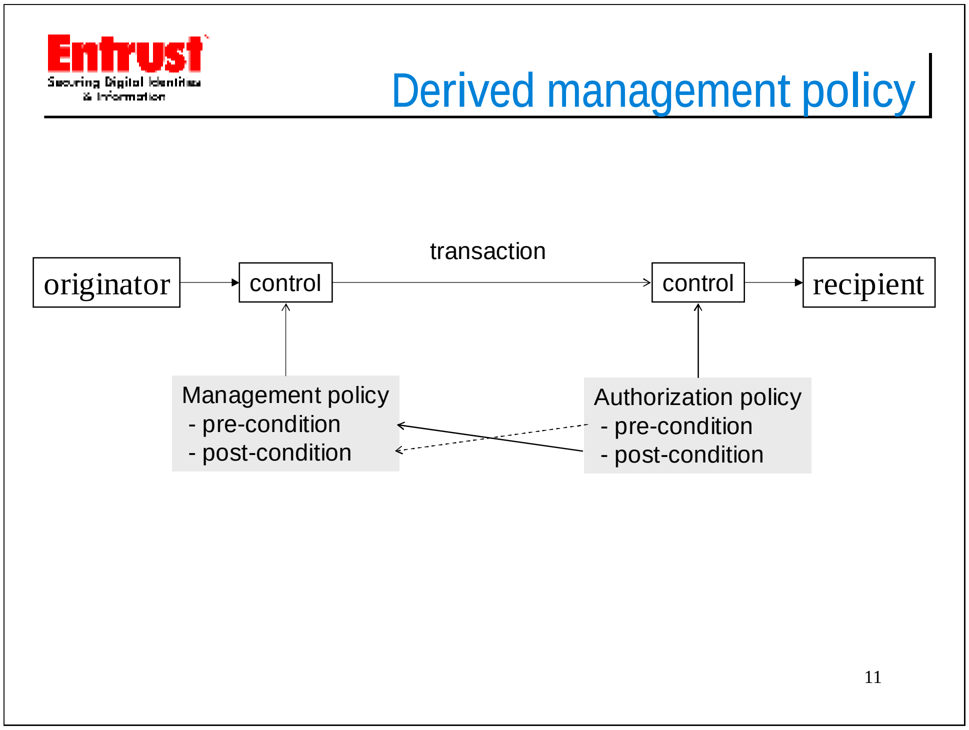
XACML adds “environment” to the set of components for the post-condition.

The combination of a resource and an action is called a permission. In the RBAC model, permissions are associated with roles.

Separation of duties adds the stipulation that the subject must not have previously acted on the transaction in a certain way.

The rights model is difficult to express in this form because it stipulates a variety of condition related to permitted actions and payment.

The post-condition, being a conjunctive sequence of predicates, is suitable for indexing policies for the purpose of storage and retrieval.



Derived management policy

Where successful invocation of a service or successful submission of a transaction requires the satisfaction of an authorization policy, the service client or transaction originator require the corresponding management policy in order to create an acceptable service request or transaction.

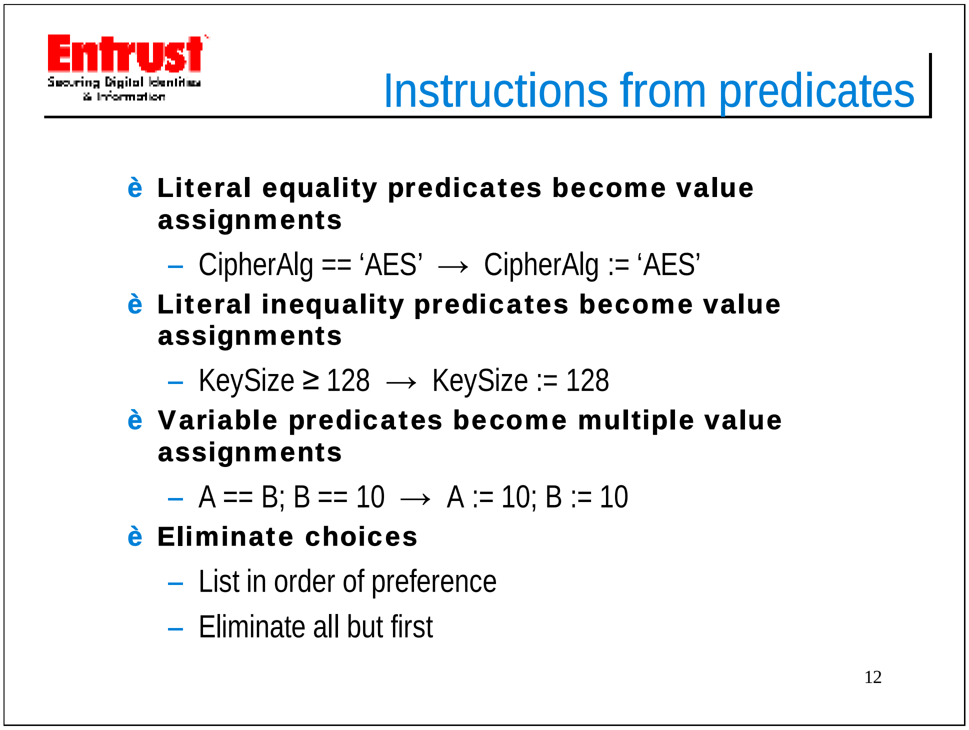
Management policy pre-condition is identical to the corresponding authorization policy's post-condition.

Management policy's post-condition is derived from the corresponding authorization policy's pre-condition by eliminating alternatives and converting predicates to assignments.

Hence we need a policy language that is amenable to derivation of a management policy from the corresponding authorization policy.

The originator may have policies that apply to the request. So, it has to merge its own management policy with that derived from the recipient's authorization policy.

Similar thing happens with any response to the transaction.



Entrust
Securing Digital Identities & Information

Instructions from predicates

è **Literal equality predicates become value assignments**

- CipherAlg == ‘AES’ → CipherAlg := ‘AES’

è **Literal inequality predicates become value assignments**

- KeySize ≥ 128 → KeySize := 128

è **Variable predicates become multiple value assignments**

- A == B; B == 10 → A := 10; B := 10

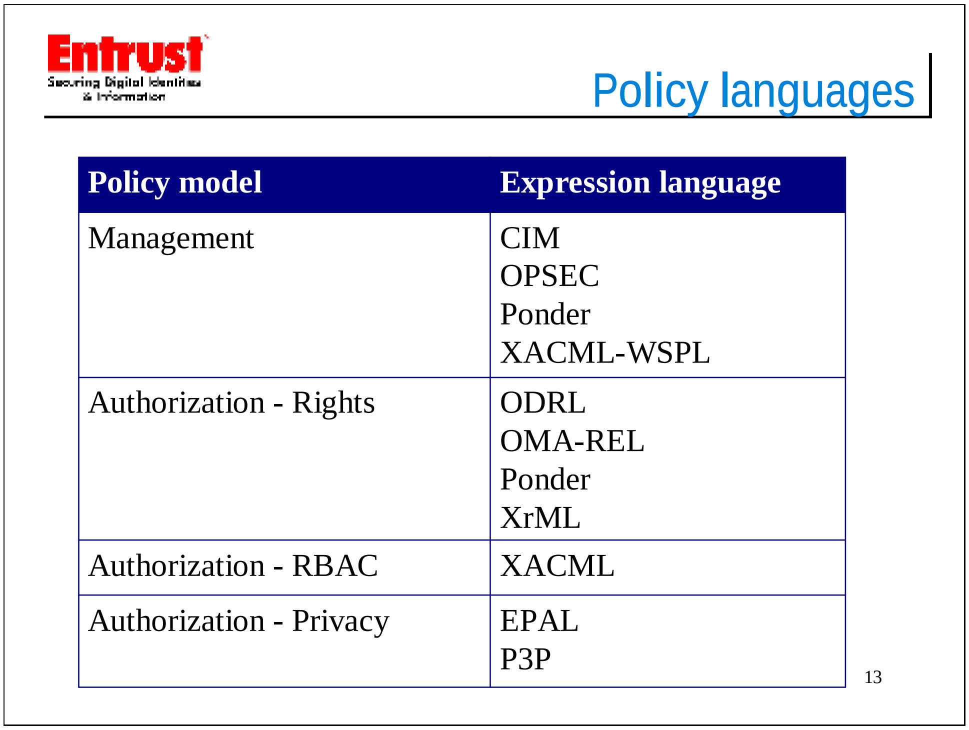
è **Eliminate choices**

- List in order of preference
- Eliminate all but first

12

Best practice is to use >=, rather than >. E.g. >= 128, not > 127.

Instructions could be converted to an executable language, such as WSBPEL.



Entrust
Securing Digital Identities & Information

Policy languages

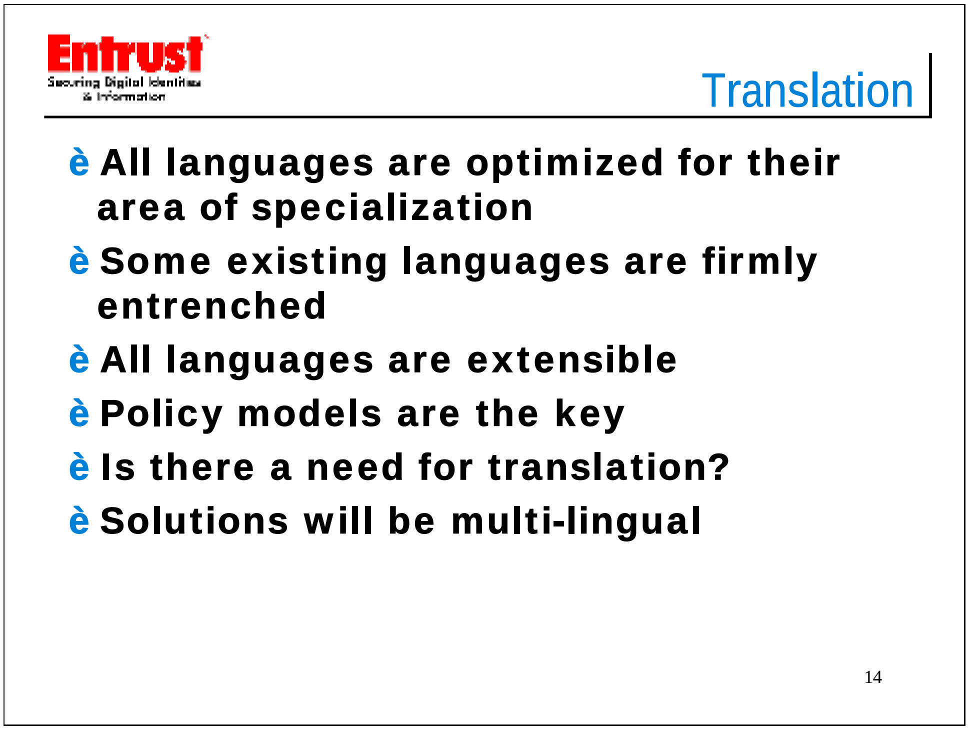
Policy model	Expression language
Management	CIM OPSEC Ponder XACML-WSPL
Authorization - Rights	ODRL OMA-REL Ponder XrML
Authorization - RBAC	XACML
Authorization - Privacy	EPAL P3P

13

Ponder can express both management and authorization policies. So can XACML. In addition XACML describes a procedure for converting an authorization policy to the corresponding management policy.

The other languages are tuned to their particular area of application.

There is no language designed specifically to address either the Chinese-wall or the separation-of-duties policy models.



Entrust
Securing Digital Identities & Information

Translation

è All languages are optimized for their area of specialization

è Some existing languages are firmly entrenched

è All languages are extensible

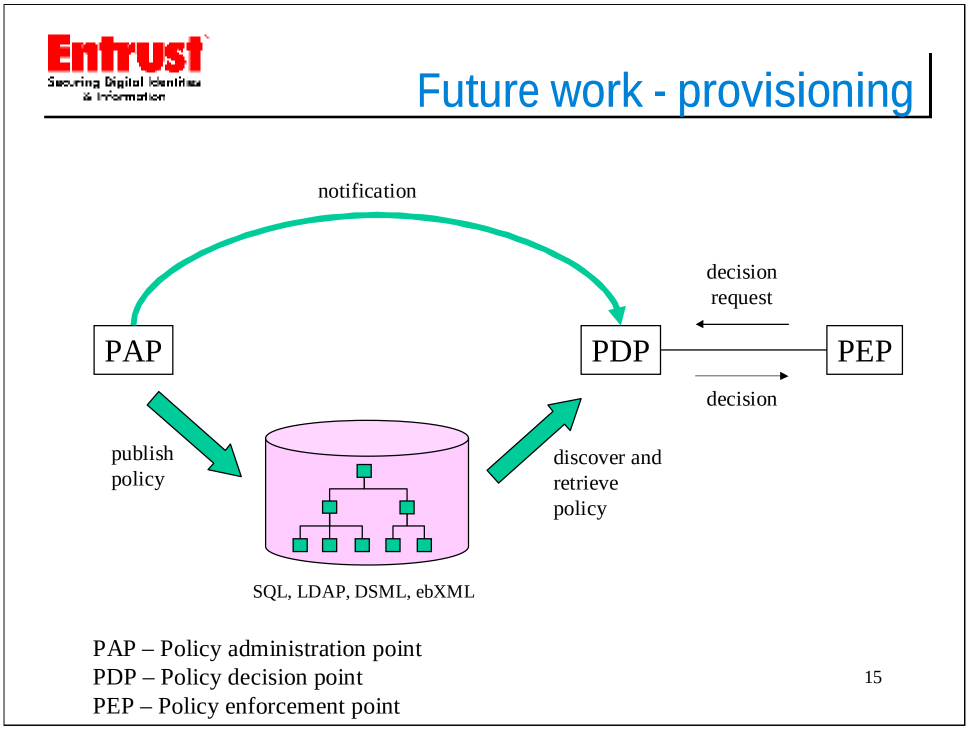
è Policy models are the key

è Is there a need for translation?

è Solutions will be multi-lingual

14

Translation is possible if and only if statements conform with one of the standard models and both languages have been profiled for that model.



Future work - provisioning

notification

decision request

PAP

PDP

PEP

decision

publish policy

discover and retrieve policy

SQL, LDAP, DSML, ebXML

PAP – Policy administration point
PDP – Policy decision point
PEP – Policy enforcement point

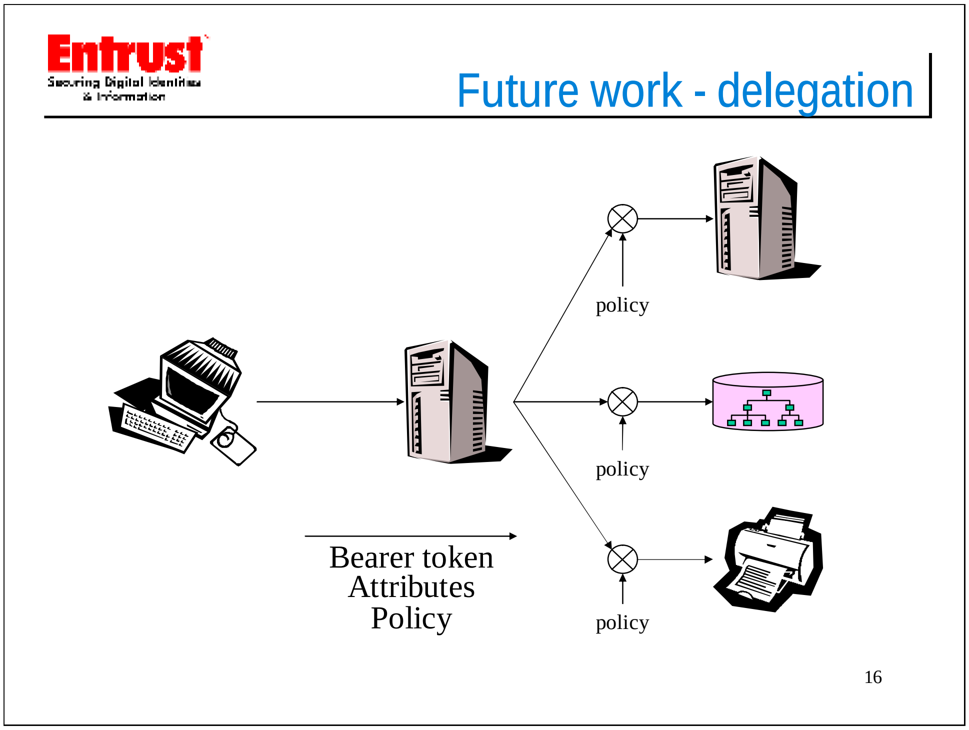
15

Rights models commonly attach the policy to the resource.

This may happen also with privacy policy.

Polices can be indexed by the post-condition (in the case of an authorization policy) or by the pre-condition (in the case of a management policy).

Inefficient to retrieve from repository at run-time.



Future work - delegation

policy

policy

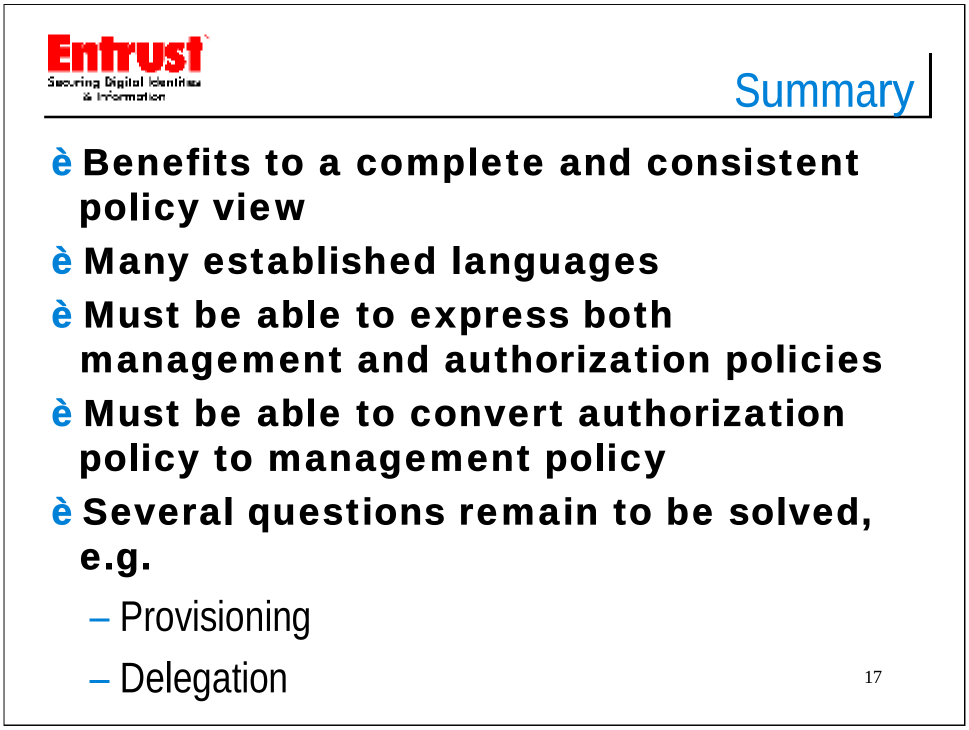
Bearer token
Attributes
Policy

policy

16

The user launches a job on a server, such as a grid computer. The grid computer needs to access software, data or hardware resources in order to complete the job. These resources are protected by policies. The policies speak in terms of the attributes of the user, not the grid computer. How can the grid computer be granted access to the resources if it is authorized by the user?

There are three main options: 1) impersonation, in which the user supplies a bearer token; 2) the user issues attributes for the computer and 3) the user issues a policy for the computer. Option 1 is the option in most common use today, but it is higher risk and accountability is poor. The rights model uses option 3. Most research directed at option 3, because it places greater control in the hands of the user. I.e. the user can grant a specific permission.



Entrust
Securing Digital Identities & Information

Summary

è **Benefits to a complete and consistent policy view**

è **Many established languages**

è **Must be able to express both management and authorization policies**

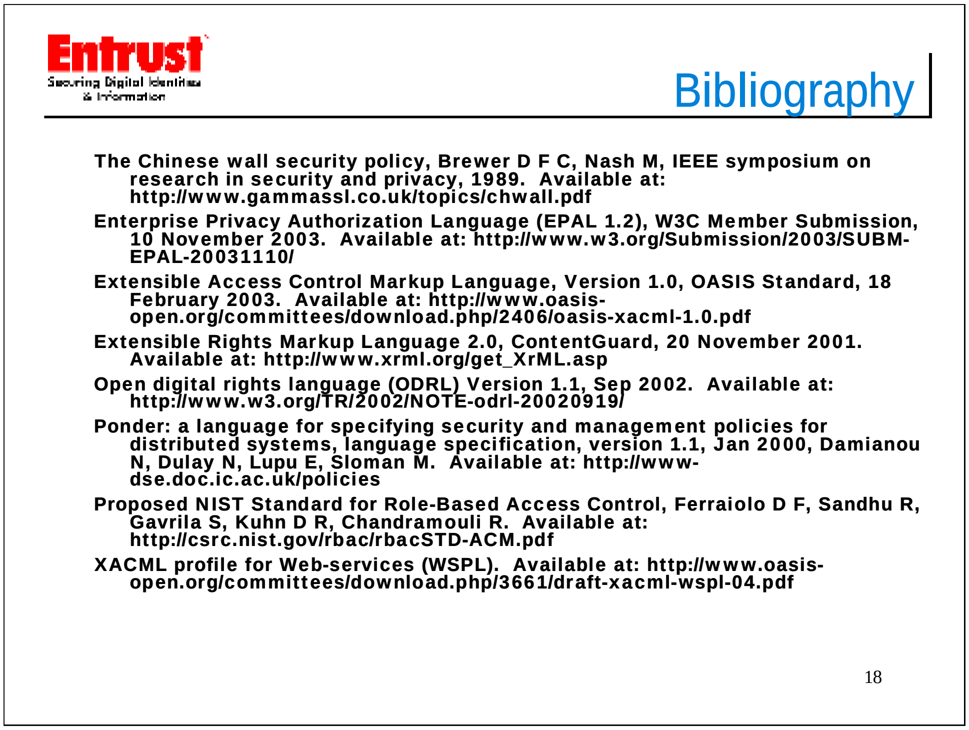
è **Must be able to convert authorization policy to management policy**

è **Several questions remain to be solved, e.g.**

– Provisioning

– Delegation

17



Entrust
Securing Digital Identities & Information

Bibliography

The Chinese wall security policy, Brewer D F C, Nash M, IEEE symposium on research in security and privacy, 1989. Available at: http://www.gammassl.co.uk/topics/chwall.pdf

Enterprise Privacy Authorization Language (EPAL 1.2), W3C Member Submission, 10 November 2003. Available at: http://www.w3.org/Submission/2003/SUBM-EPAL-20031110/

Extensible Access Control Markup Language, Version 1.0, OASIS Standard, 18 February 2003. Available at: http://www.oasis-open.org/committees/download.php/2406/oasis-xacml-1.0.pdf

Extensible Rights Markup Language 2.0, ContentGuard, 20 November 2001. Available at: http://www.xrml.org/get_XrML.asp

Open digital rights language (ODRL) Version 1.1, Sep 2002. Available at: http://www.w3.org/TR/2002/NOTE-odrl-20020919/

Ponder: a language for specifying security and management policies for distributed systems, language specification, version 1.1, Jan 2000, Damianou N, Dulay N, Lupu E, Sloman M. Available at: http://www-dse.doc.ic.ac.uk/policies

Proposed NIST Standard for Role-Based Access Control, Ferraiolo D F, Sandhu R, Gavrila S, Kuhn D R, Chandramouli R. Available at: http://csrc.nist.gov/rbac/rbacSTD-ACM.pdf

XACML profile for Web-services (WSPL). Available at: http://www.oasis-open.org/committees/download.php/3661/draft-xacml-wspl-04.pdf