



Unifying framework for Identity management

Breakfast seminar Security-Assessment.com



Stephan Overbeek

2006-03-28

Where it all comes together:

Disclaimer

- + This is a slide pack that supports a narrative and needs to be accompanied by the presentation.
- + This slide pack is NOT self-explanatory.
- + If you were NOT present at this presentation, please do NOT use any of this presentation, because it is unlikely you will use it appropriately.
- + Please contact me (see last slide) if you want to understand the ideas in this slide pack.

Overview

- + Identity management
 - **Purpose**
 - **Context**

- + Unifying Model for Identity Management
 - **Explanation**
 - **Usage and applicability**

- + Discussion

Identity management – Concepts – Confusion

Access control **Single Sign-On** **Accountability**
PKI **CRM** **Auditability** **Verification**
Compliance **Validation** **User management** **Enrolment**
Authorisations **Provisioning** **Certificates**
Identification **Tokens** **Trust** **Permissions**
Password **Workflow** **Registration** **Privacy**
Anonymity **Biometrics** **Credentials**
Federation **Smart cards** **Access control lists**

Identity management – definition

Identity Management

The policies, rules, processes and systems involved in ensuring that only known, **authorised Identities gain access** to networks and systems and the information contained therein.

From AGIMO's Glossary:
<http://www.agimo.gov.au/infrastructure/authentication/agaf/glossary/i#IdentityManagement>

Identity management – access management

Why – Purpose:

- + Access management – before the act
 - **Who has access to what?**
 - **Ensure authorised people have access and unauthorised people do not have access**

- + Accountability – after the act
 - **Who has done what?**
 - **Ensure relation from individuals to actions**

Context of identity management



Applications

**Identity management
(authorisation, identification,
authentication)**

**Services
(networking, workflow,
device security, ...)**

**Identity-
enabled
applications**

Context of identity management



Applications

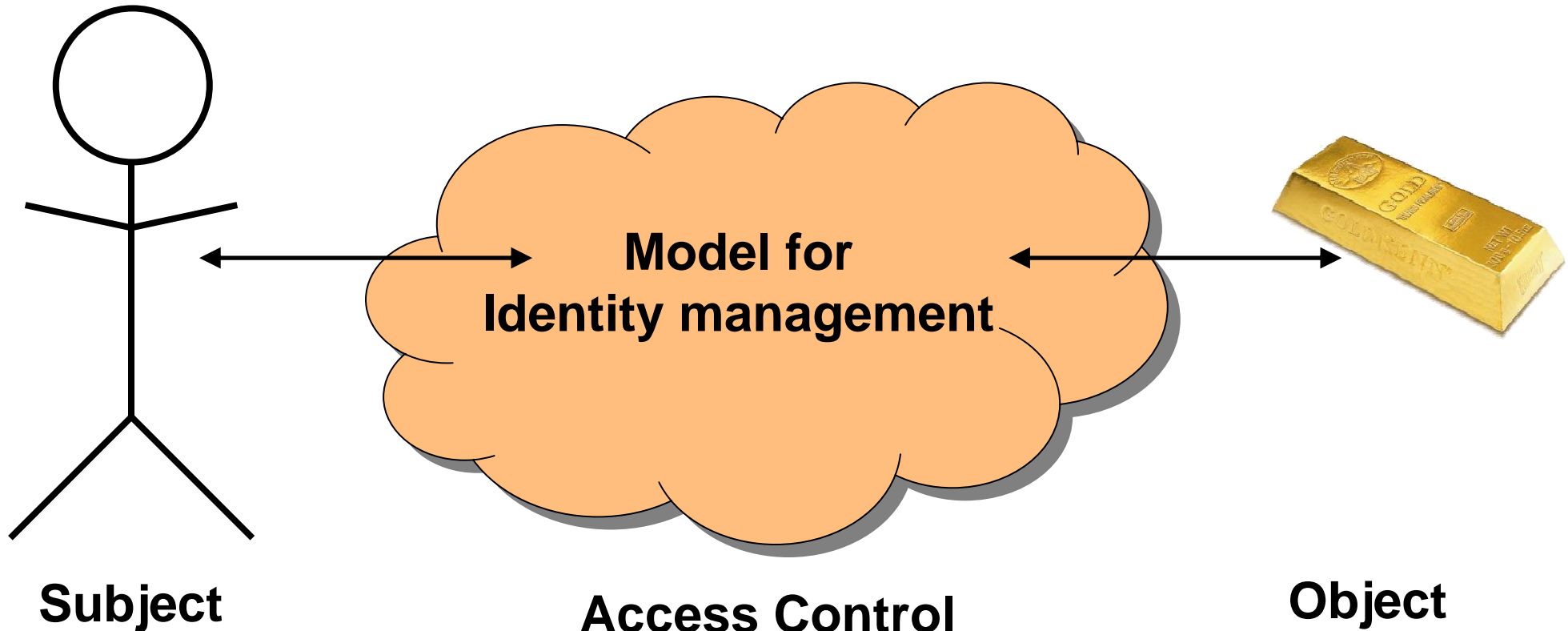
**Identity management
(authorisation, identification,
authentication)**

**Services
(networking, workflow,
device security, ...)**

**Services to
applications**

Identity management – model

*



**Anyone/anything
requesting access**

Any type of access

Assets (valuable)

Subjects and Objects

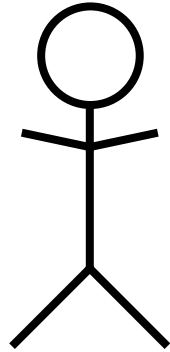
Subjects:

+ Individuals:

- **Employees**
- **Users**
- **Customers**
- **Partners**
- **Suppliers**
- **etc.**

+ Agents:

- **Processes**
- **Software**
- **Hardware**
- **etc.**



Objects:

+ Physical (access):

- **Countries**
- **Premises**
- **Buildings**
- **Vaults**
- **etc.**

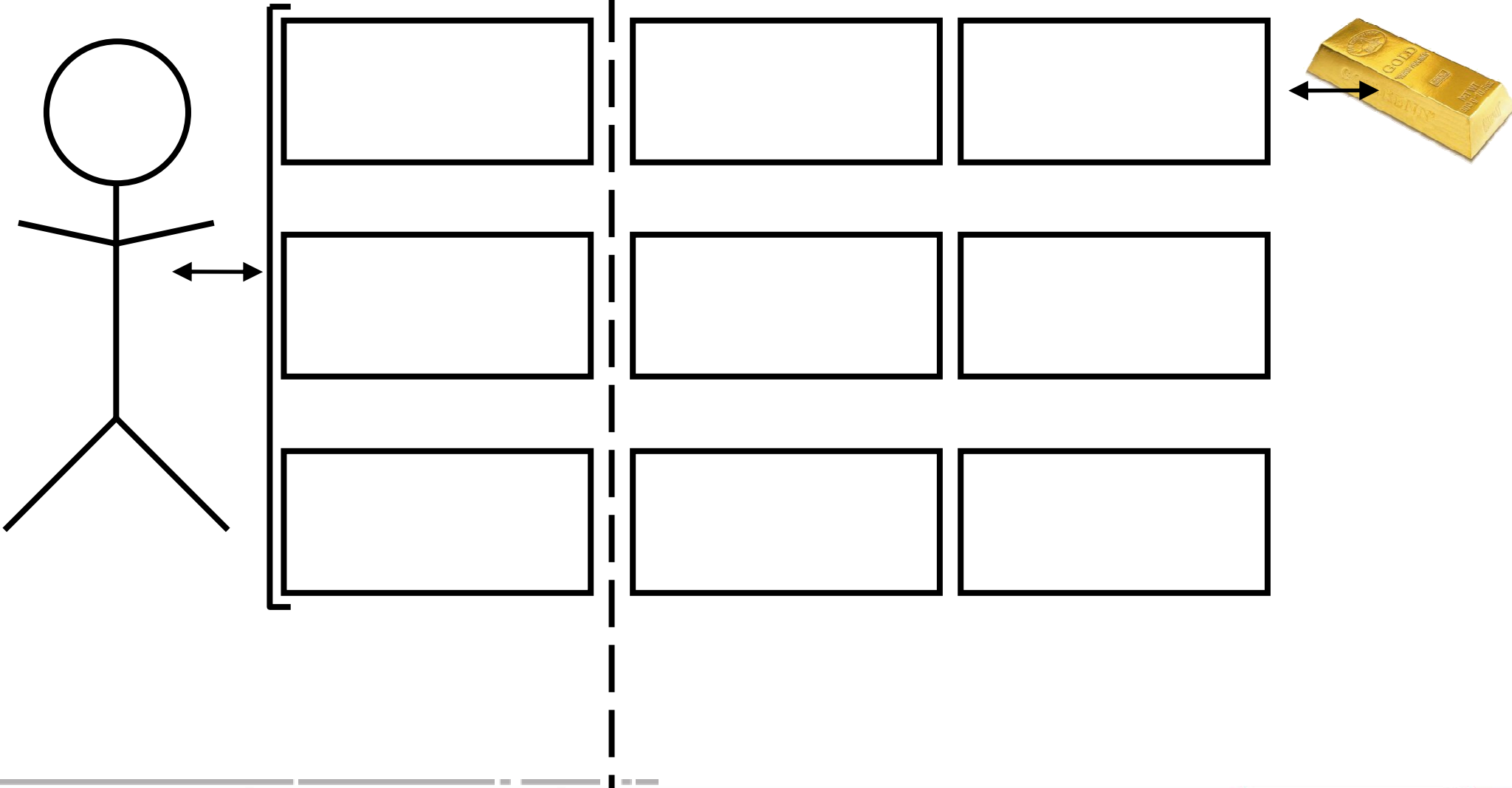


+ Logical (access):

- **Processes**
- **Databases**
- **Applications**
- **Devices**
- **etc.**

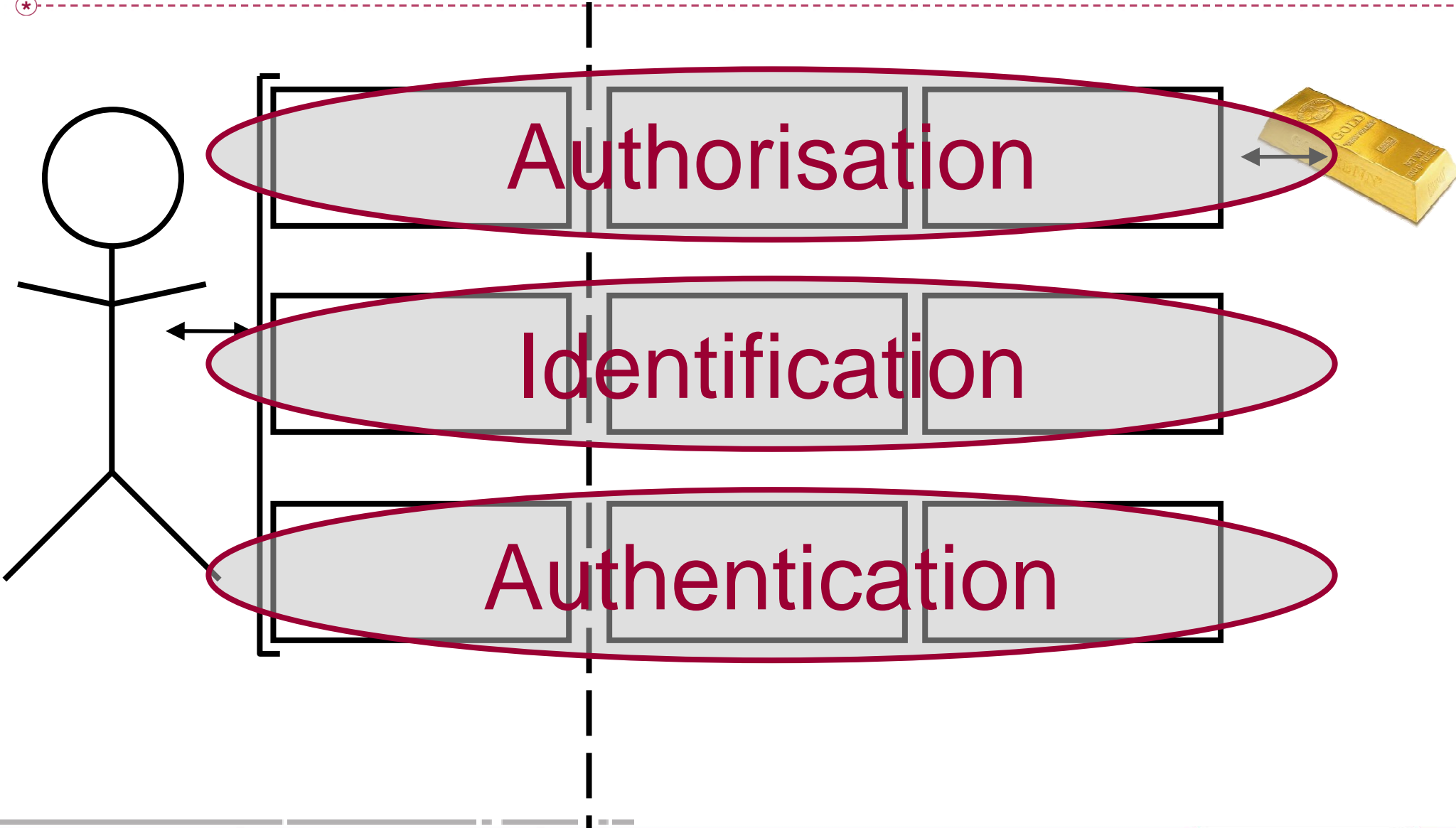
Model – components

*



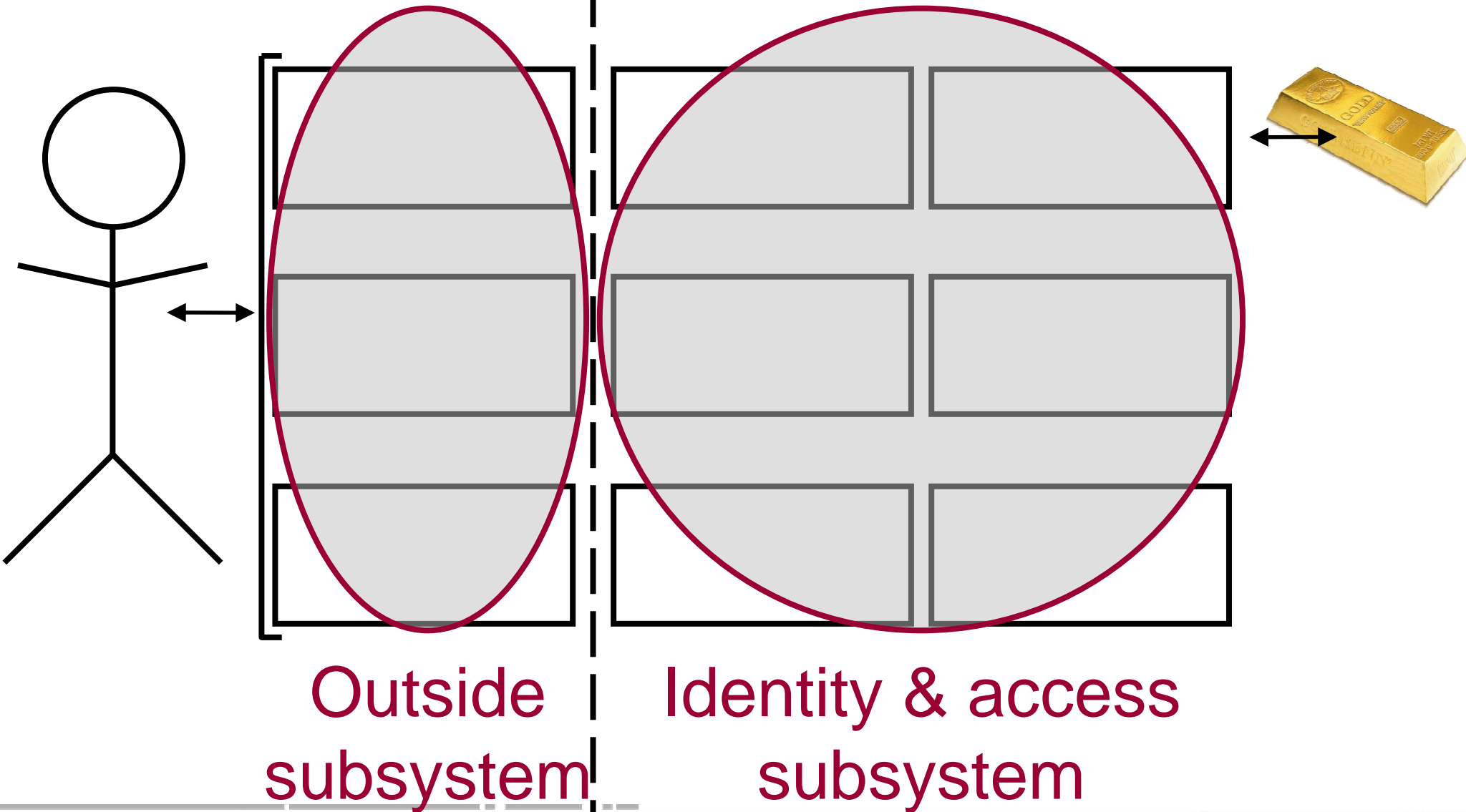
Model – three layers

*



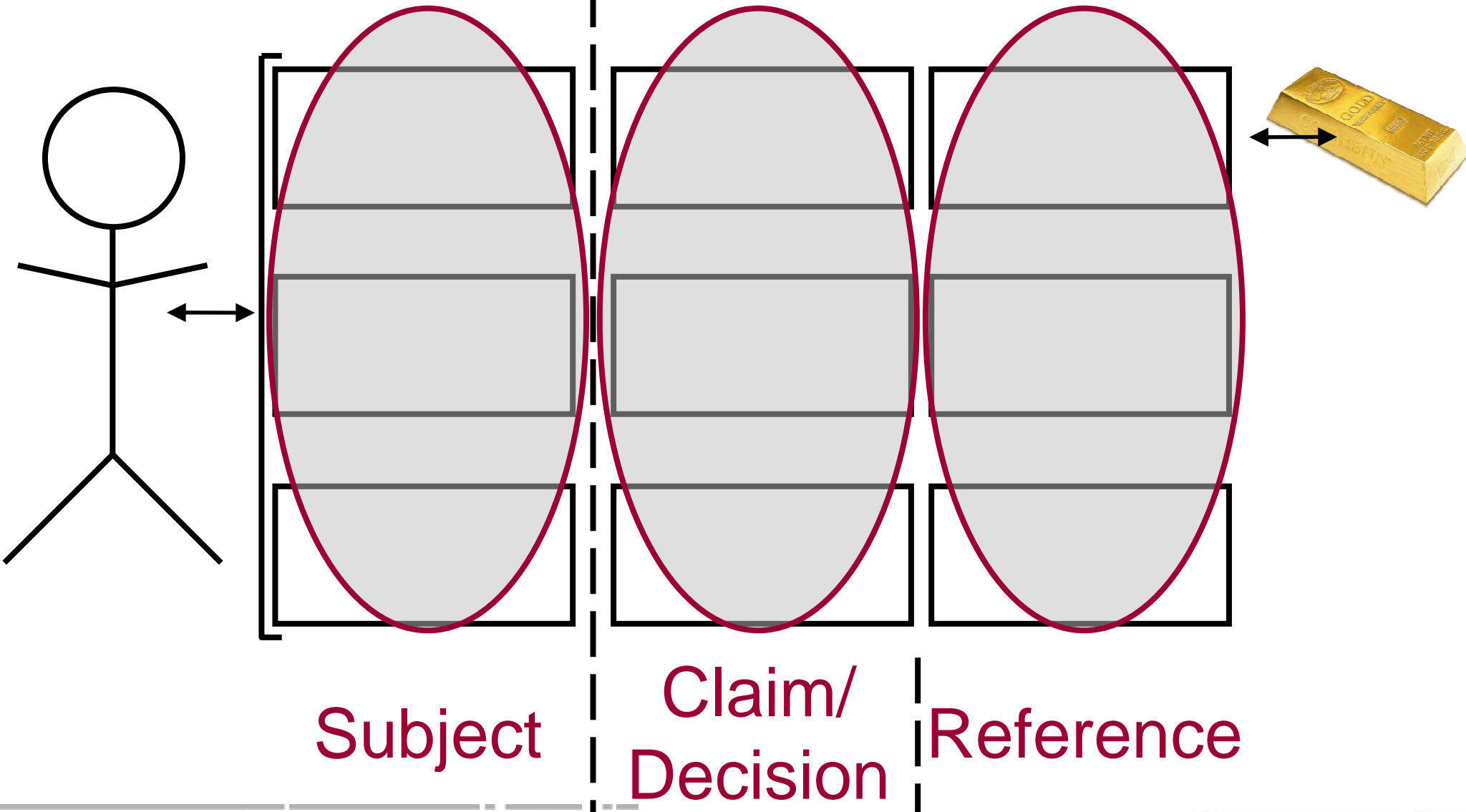
Model – identity & access subsystem

*



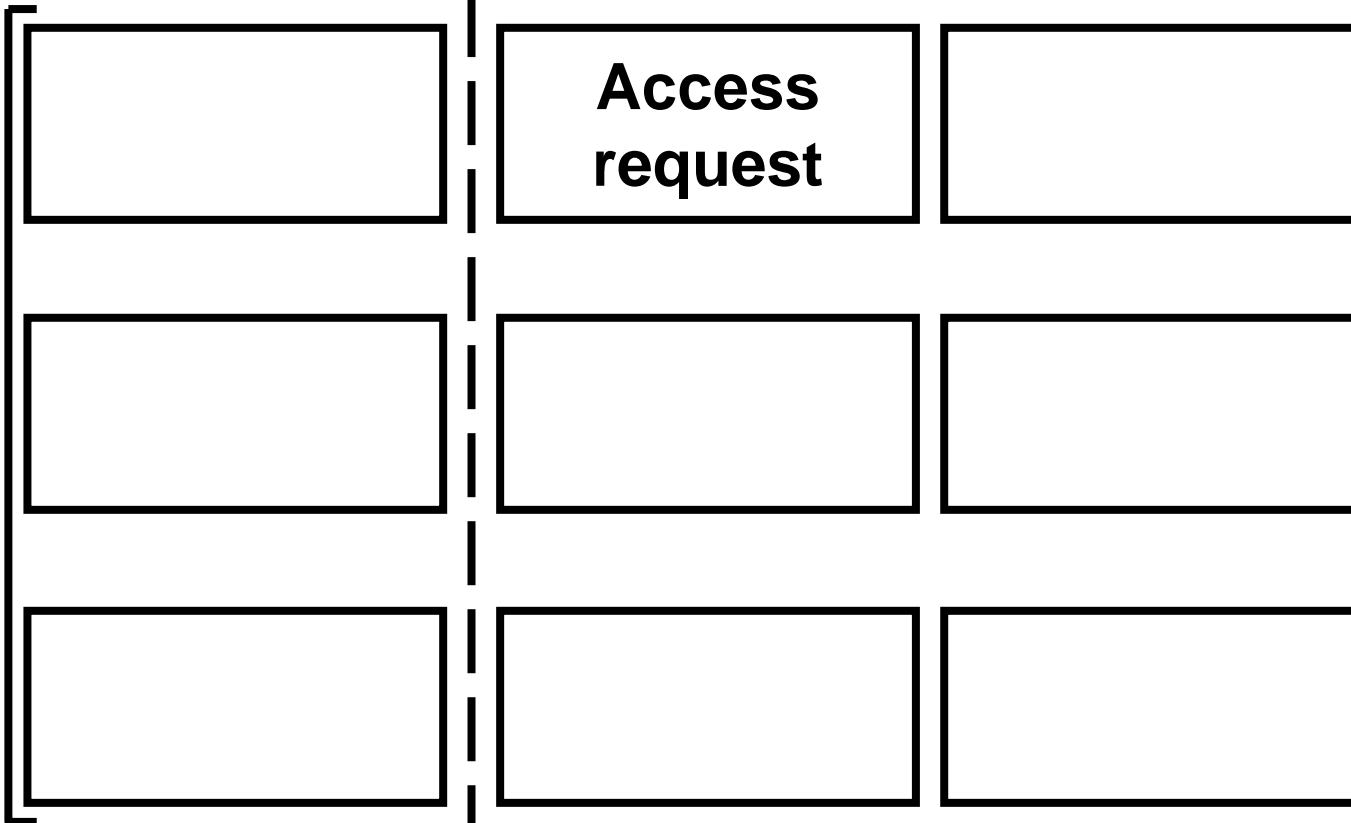
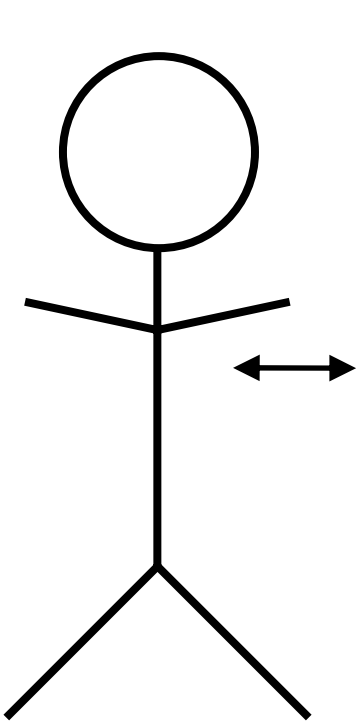
Model – three columns

*



Identity management model – access request

*



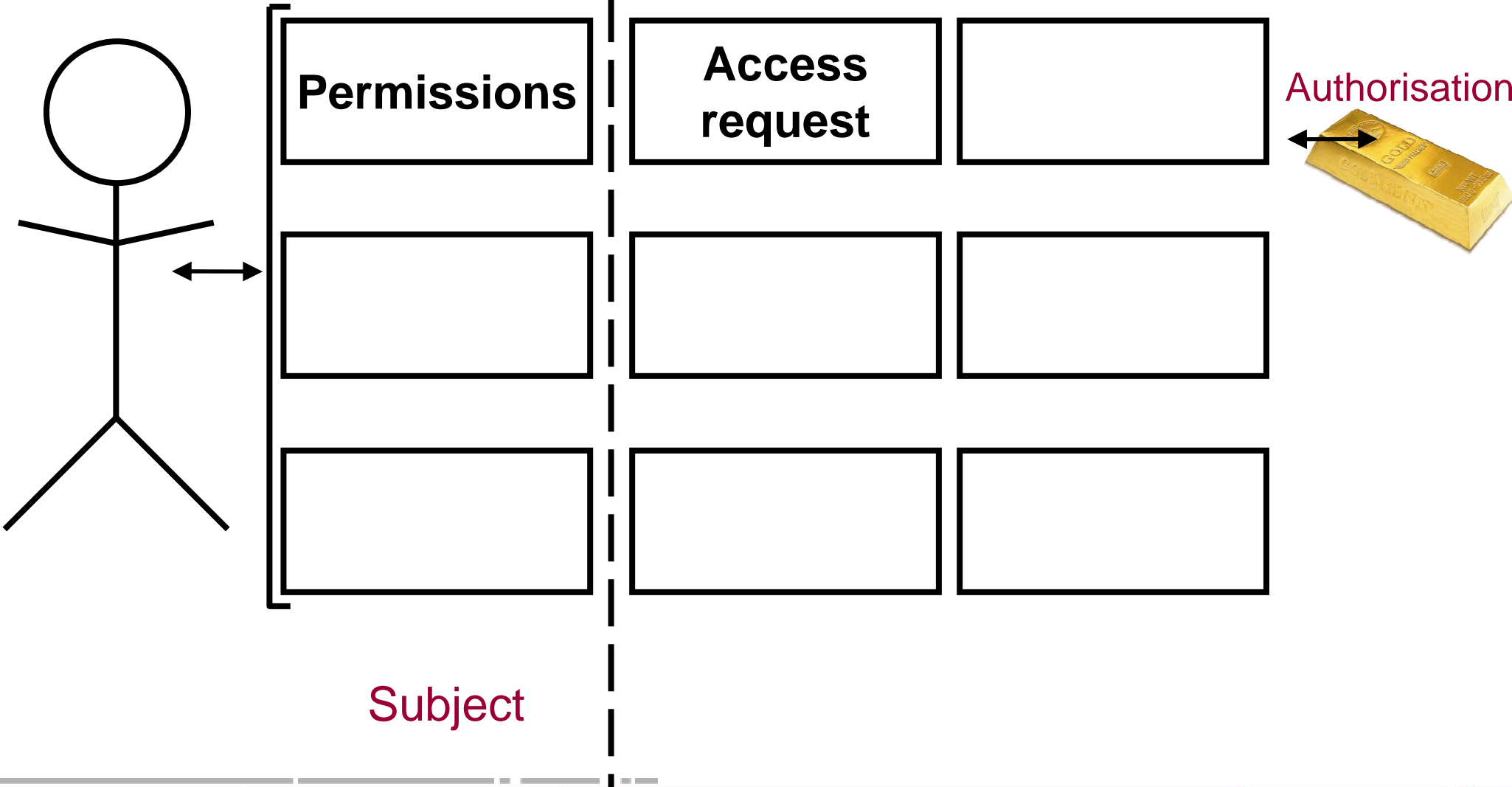
Authorisation



Claim/
Decision

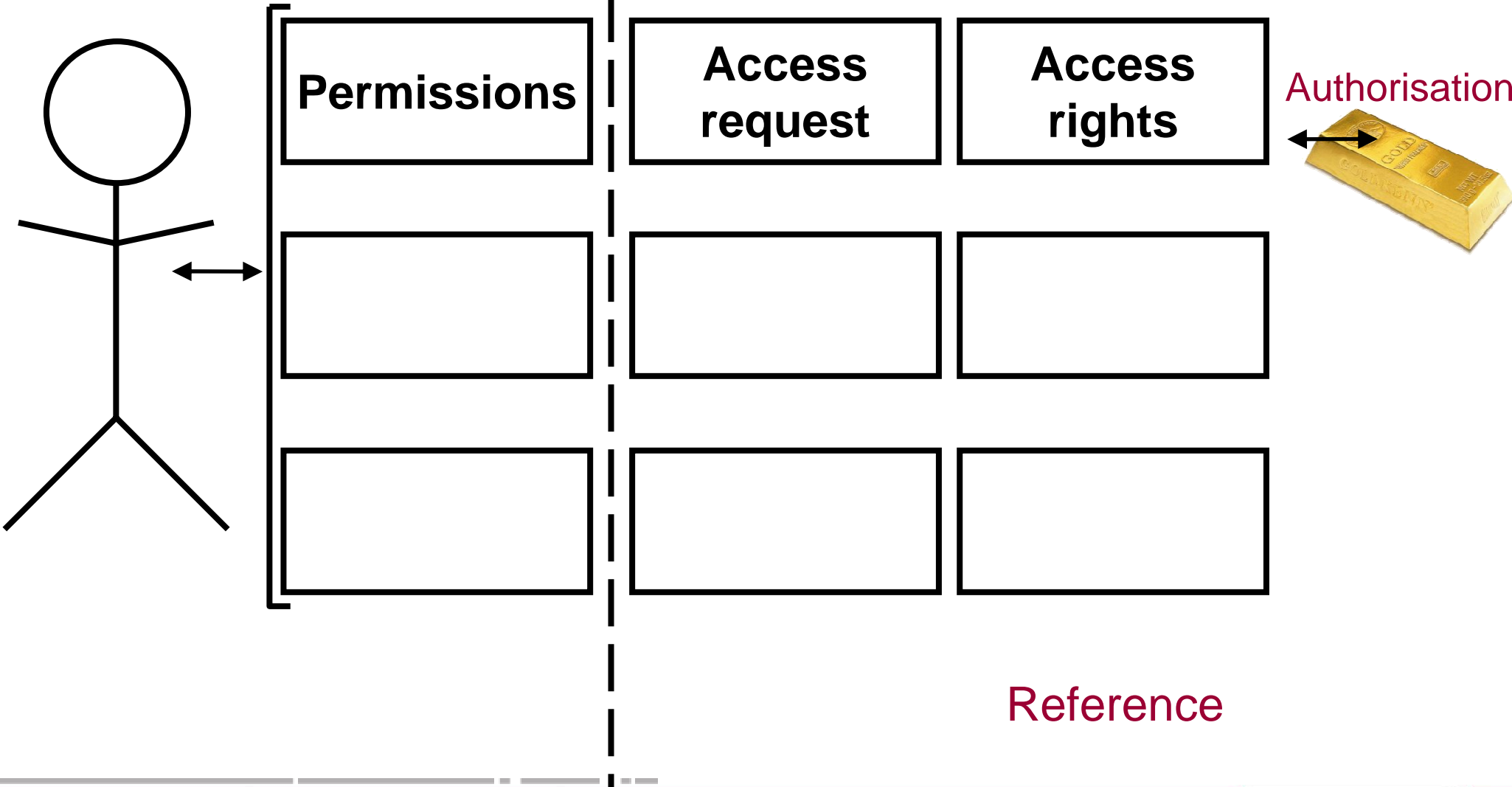
Identity management model – permissions

*



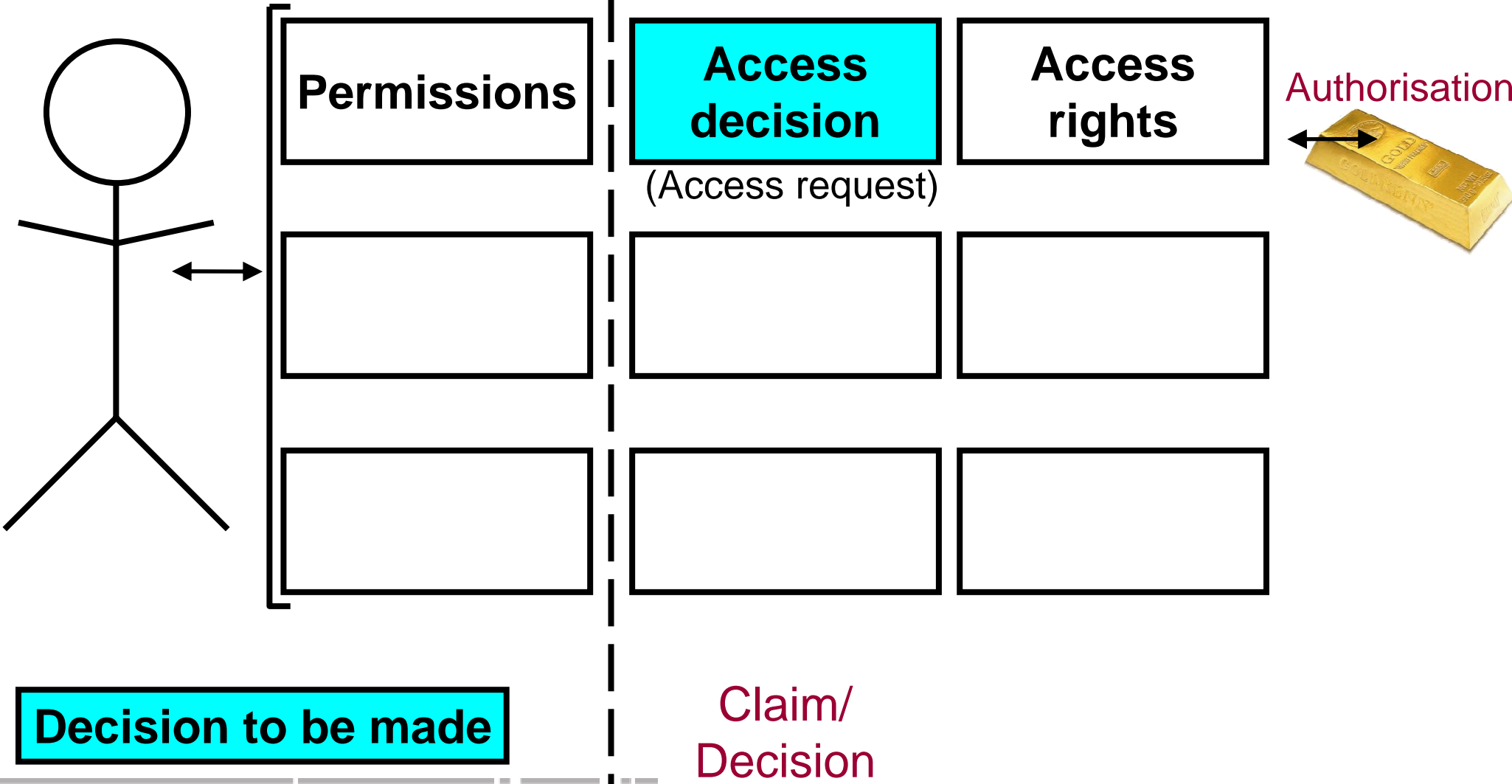
Identity management model – access rights

*



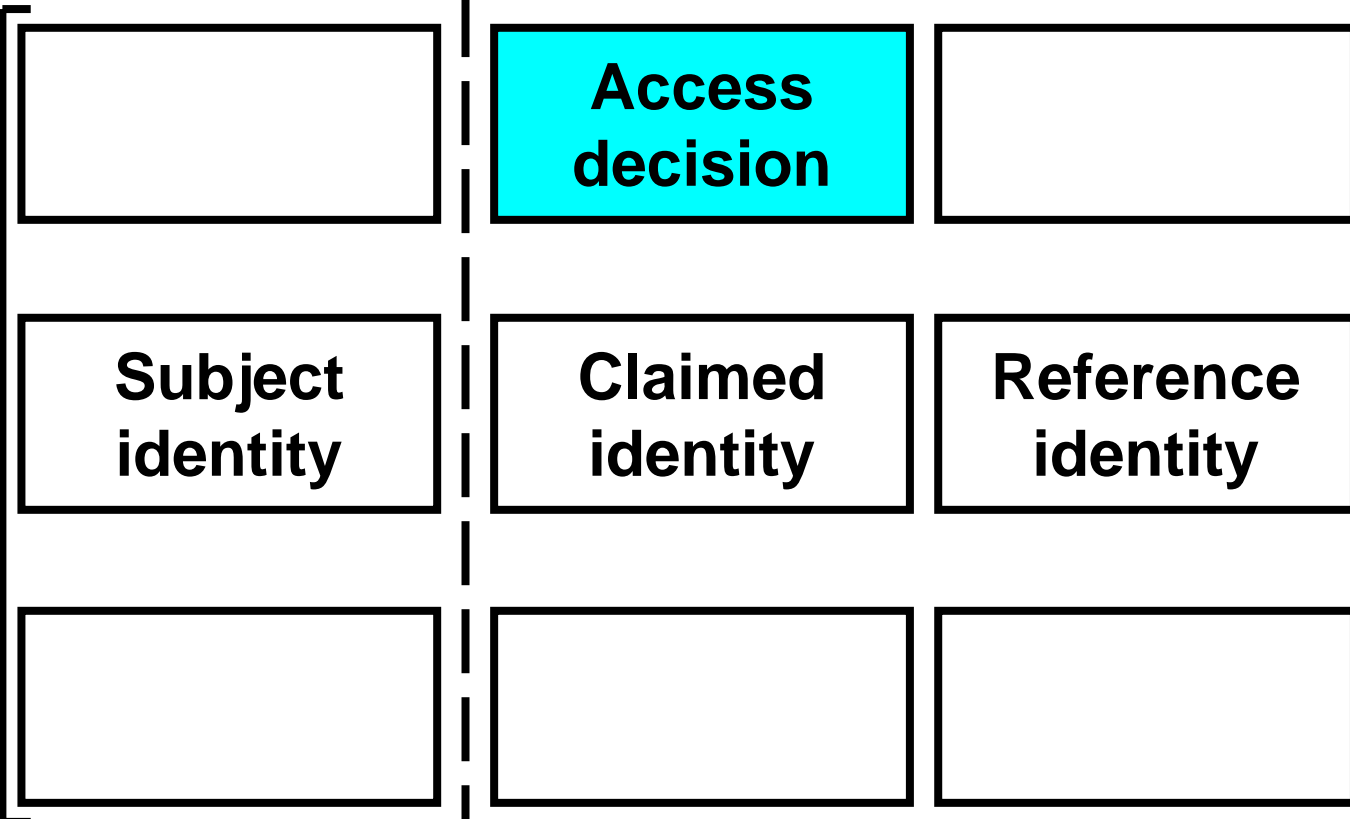
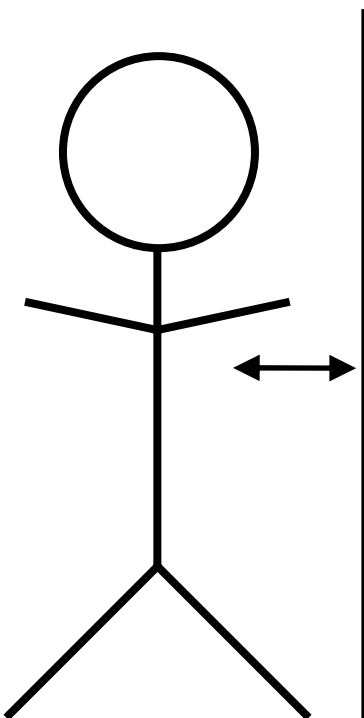
Identity management model – access decision

*



Identity management model – subject uniqueness

*



Identification

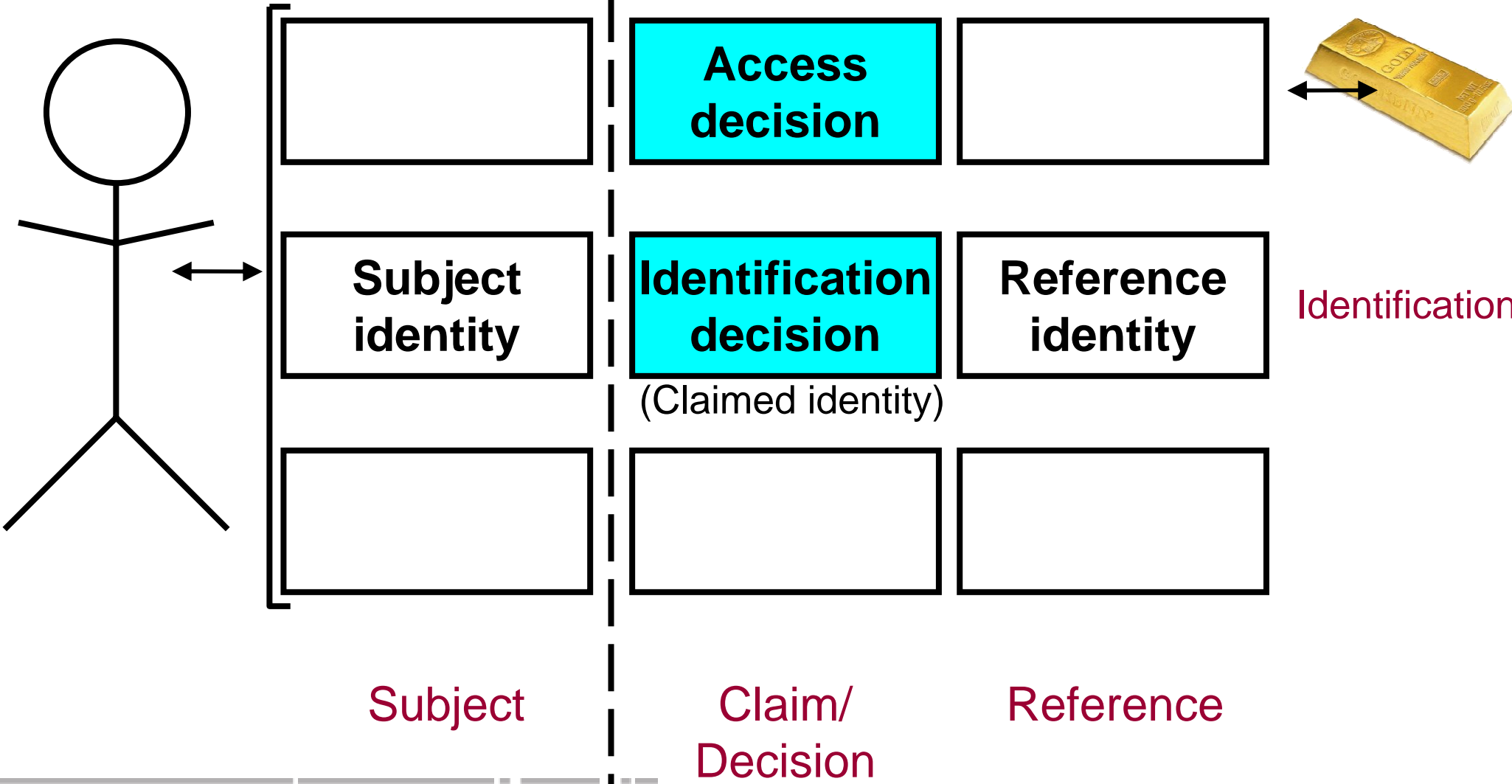
Subject

Claim/
Decision

Reference

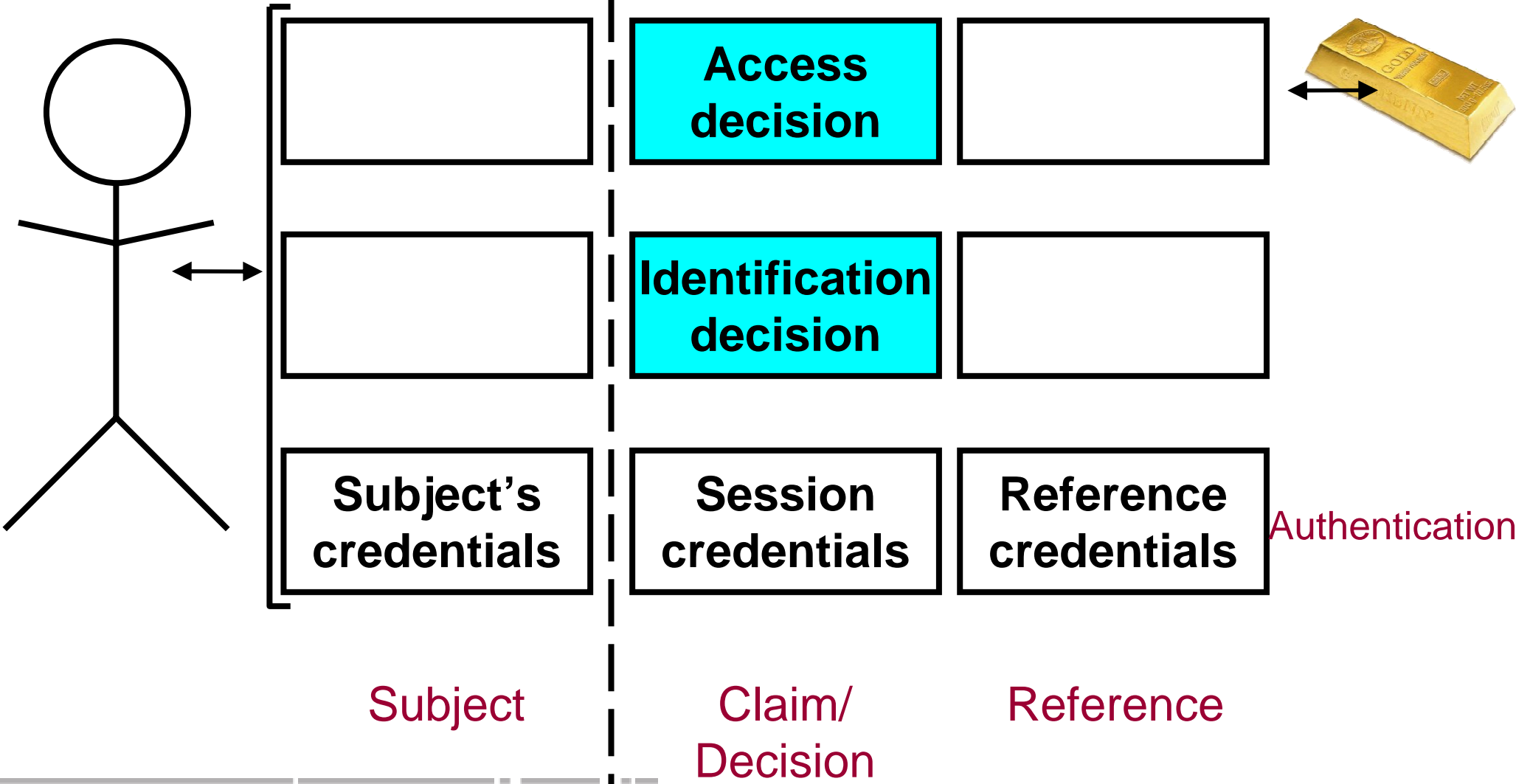
Identity management model – subject uniqueness

*



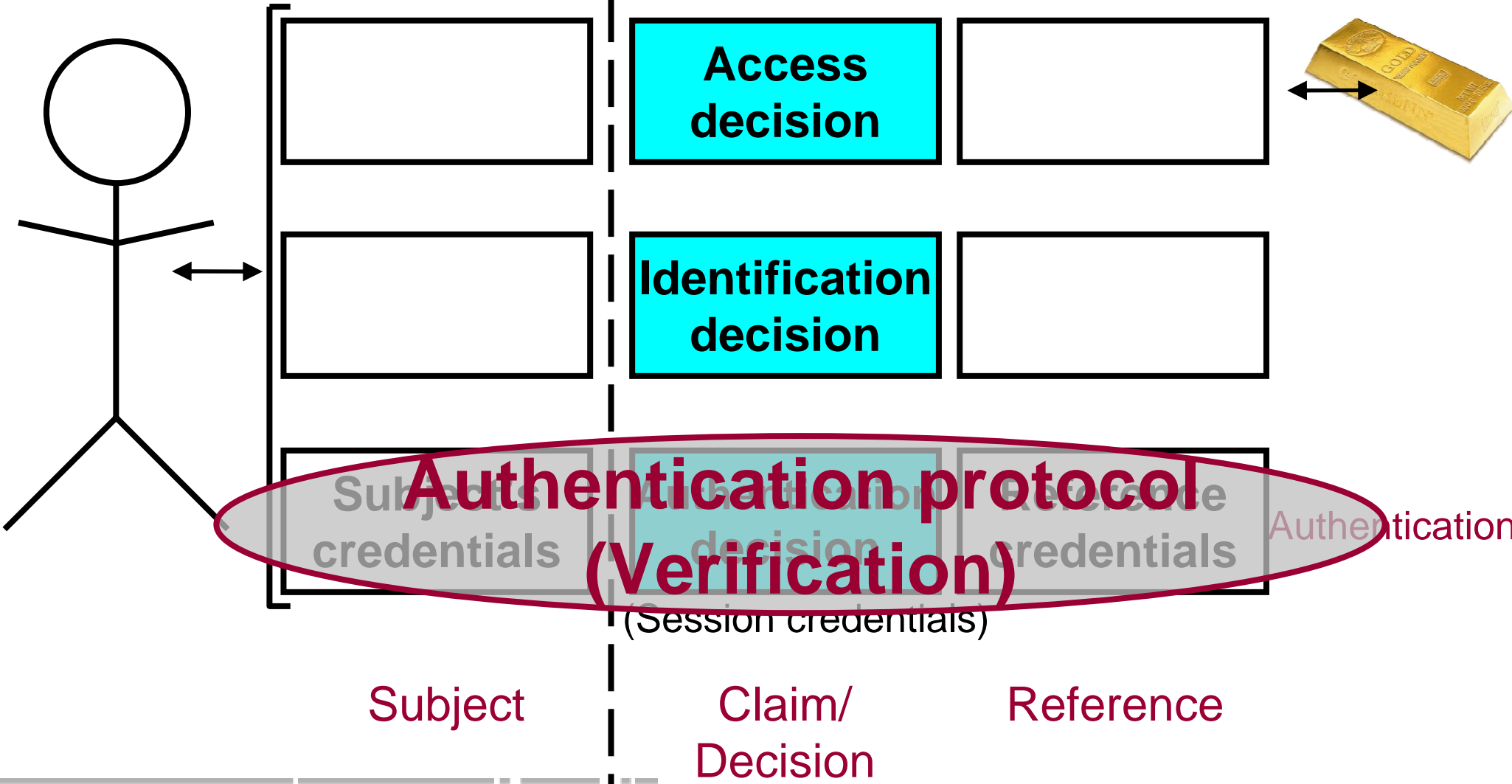
Identity management model – subject credentials

*



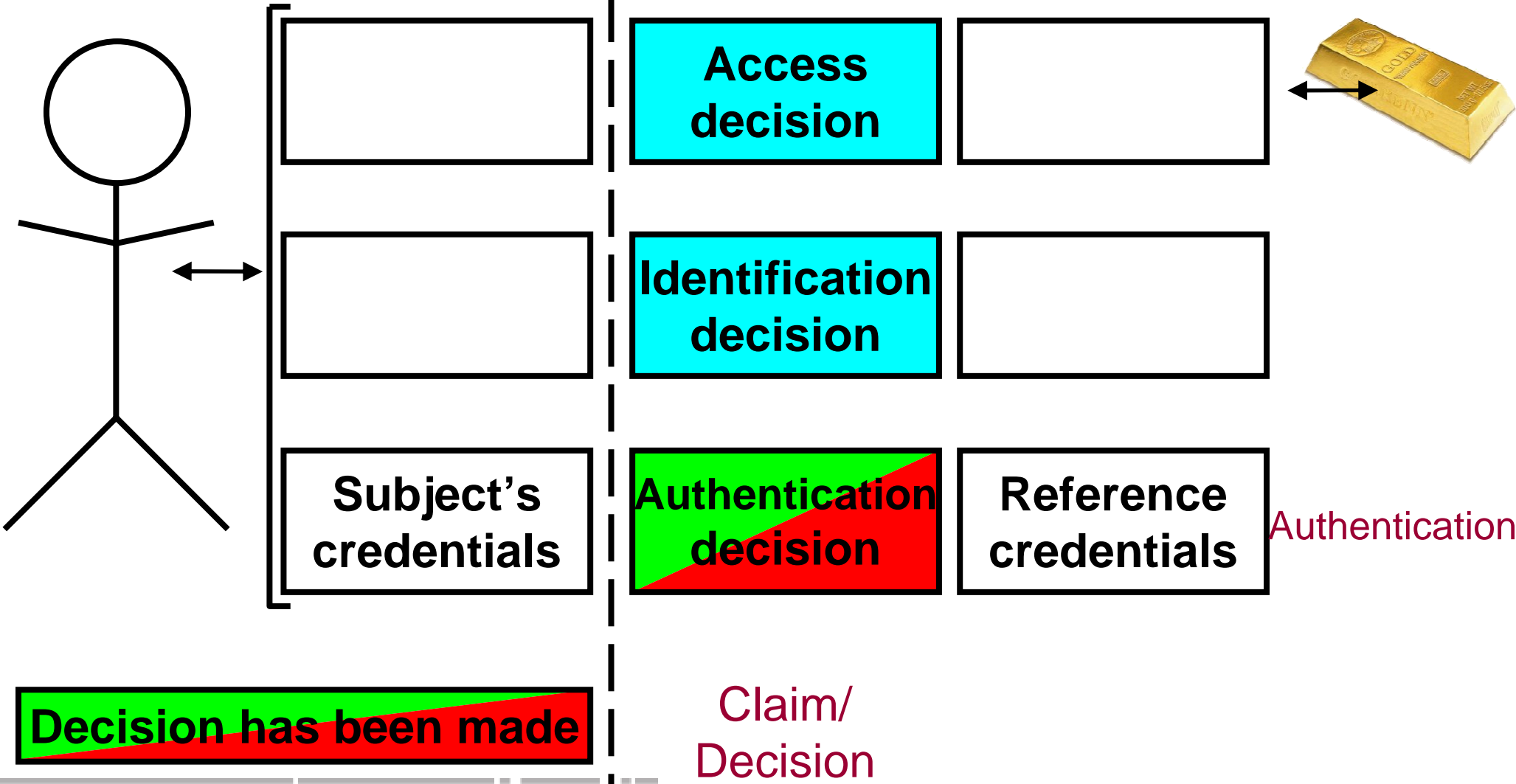
Identity management model – verification of credentials

*



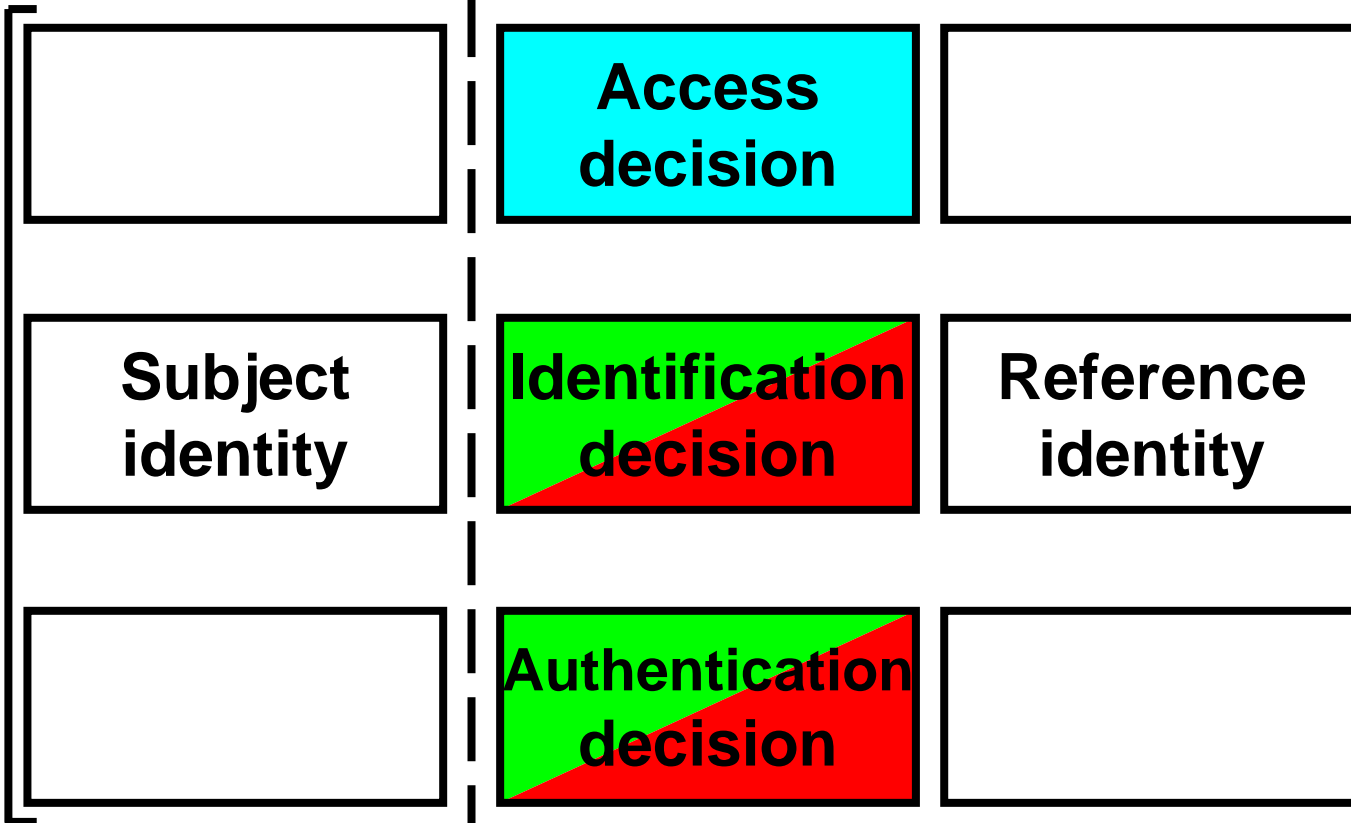
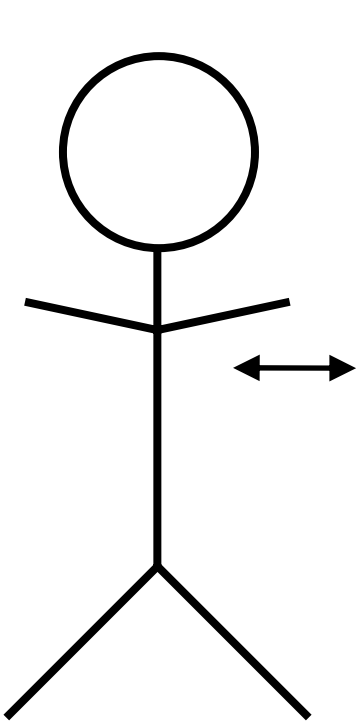
Identity management model – credentials verified

*



Identity management model – identity verified

*

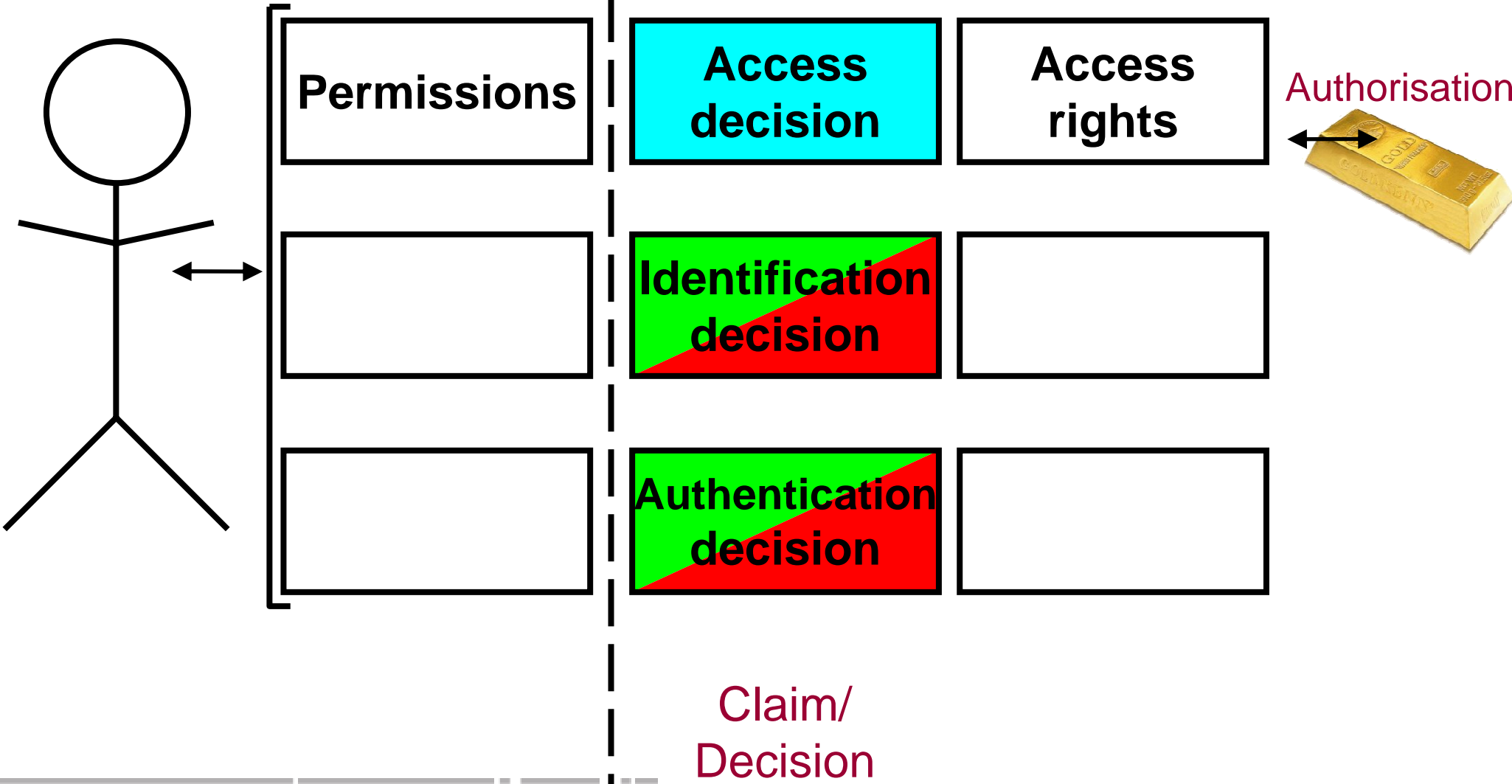


Identification

Claim/
Decision

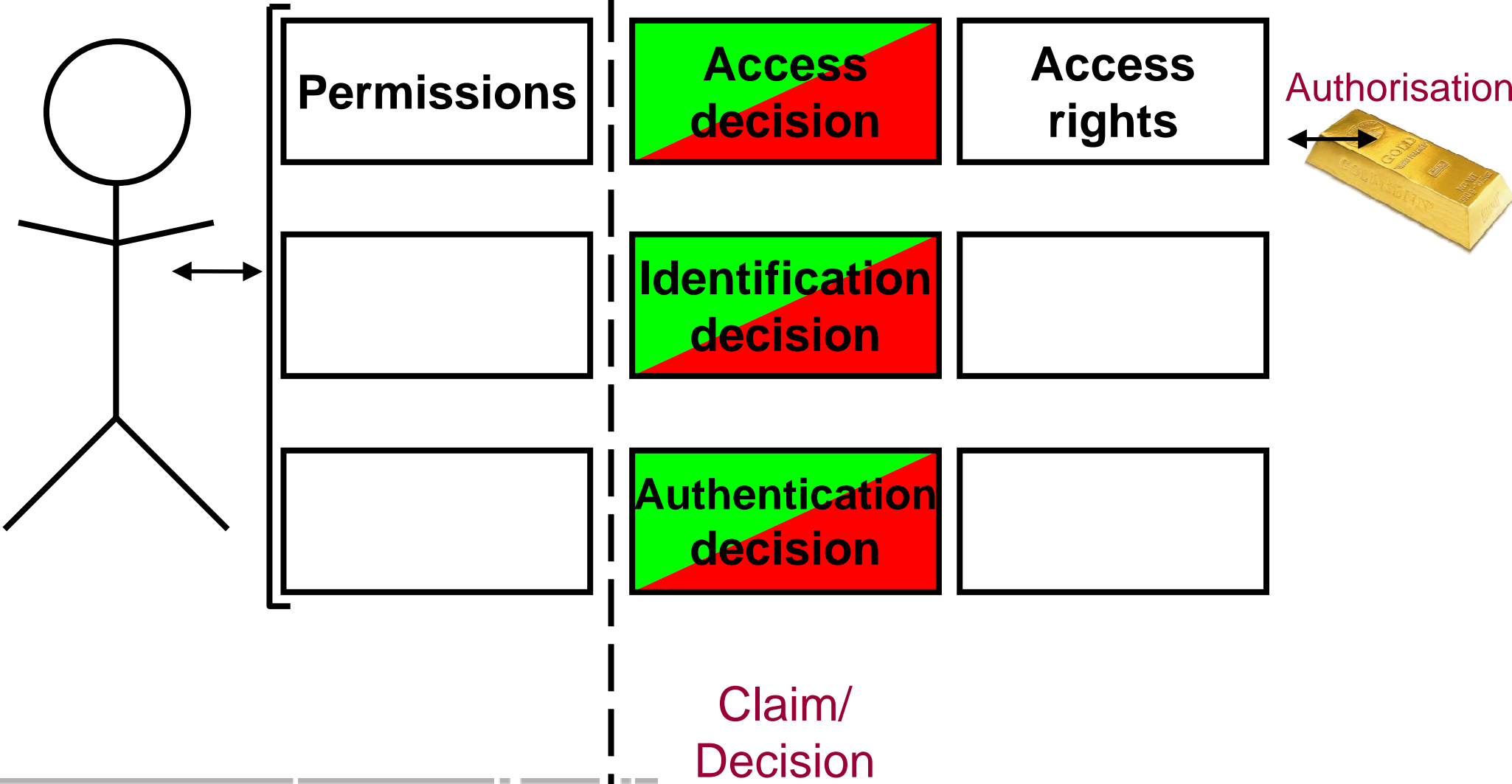
Identity management model – access decision / rights

*

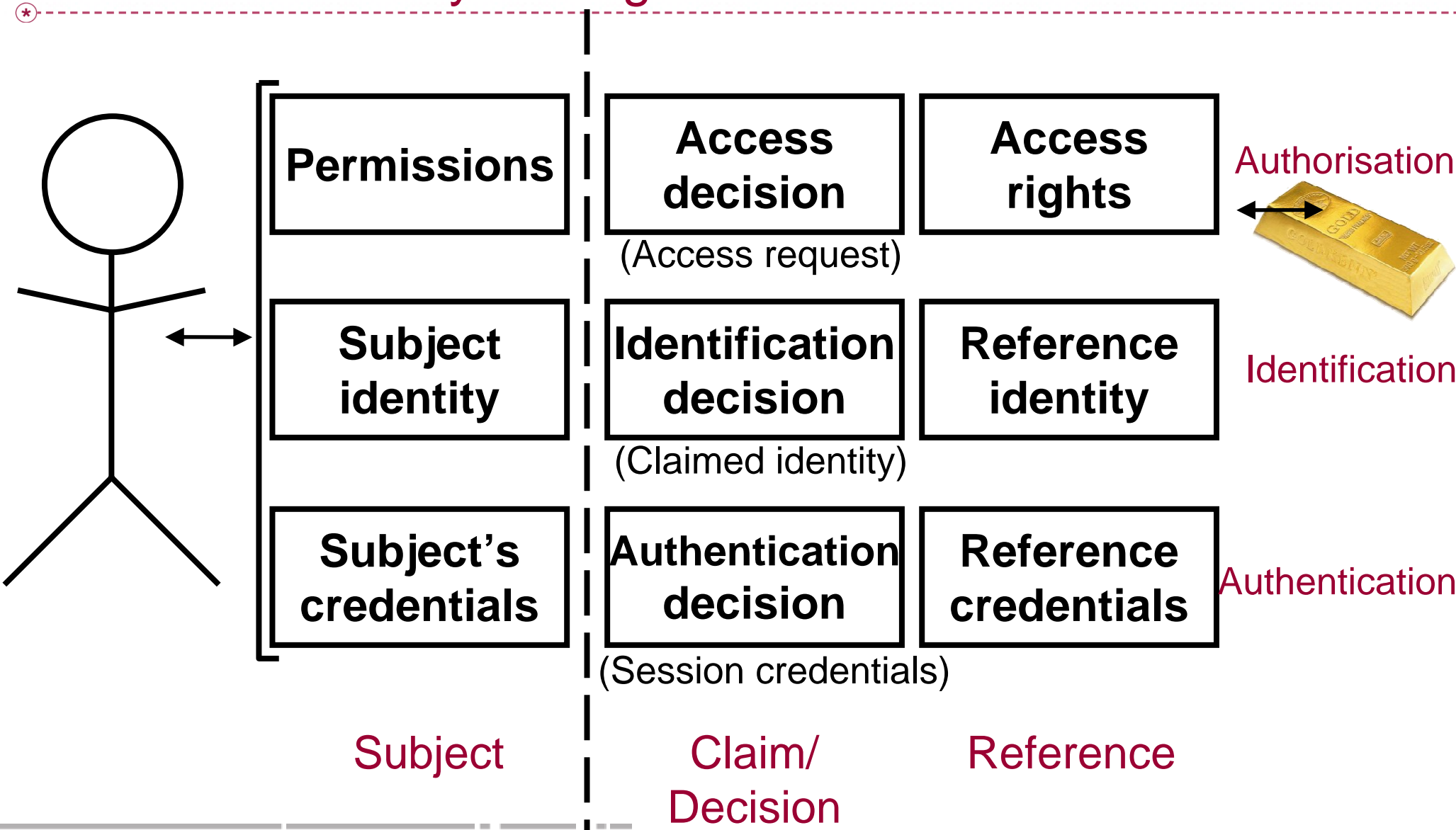


Identity management model – access decision

*

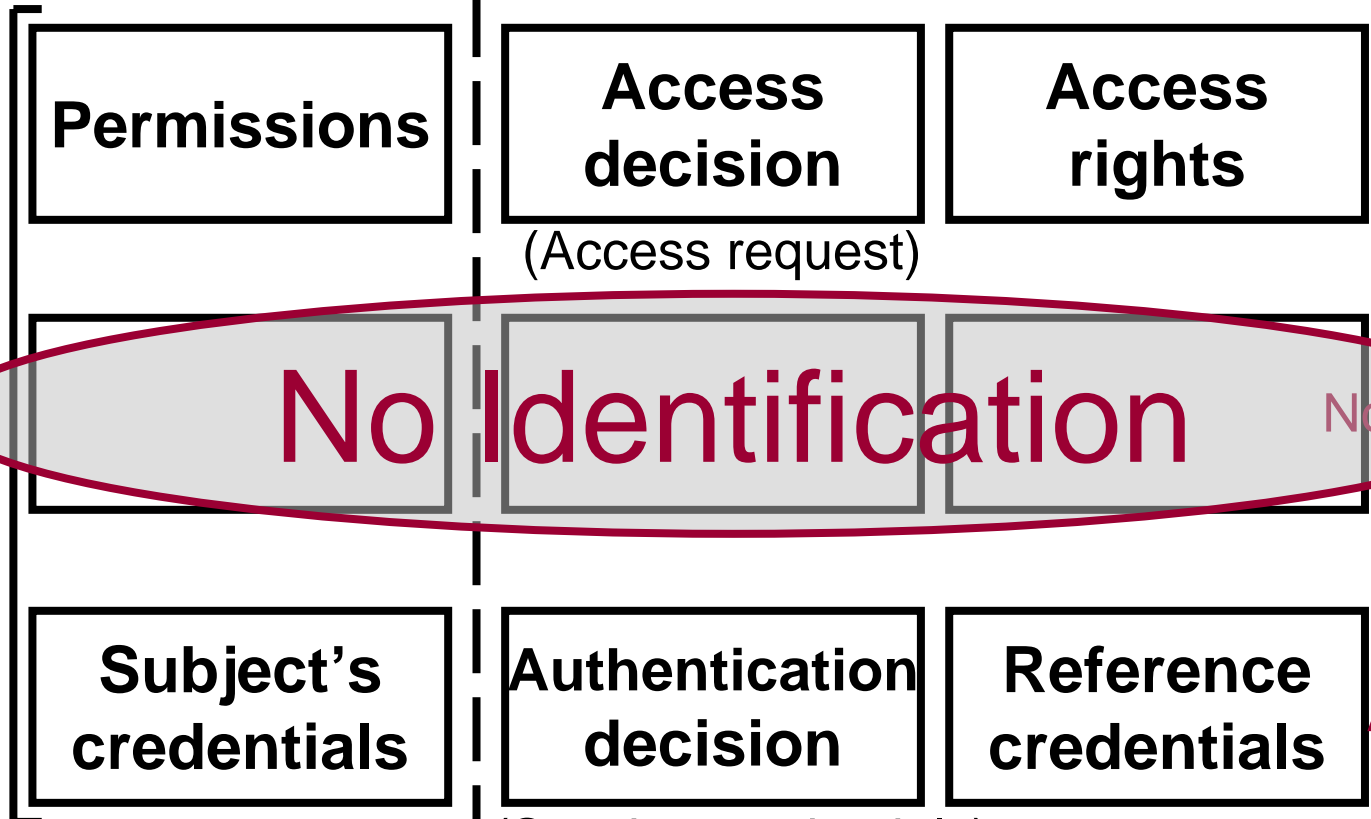
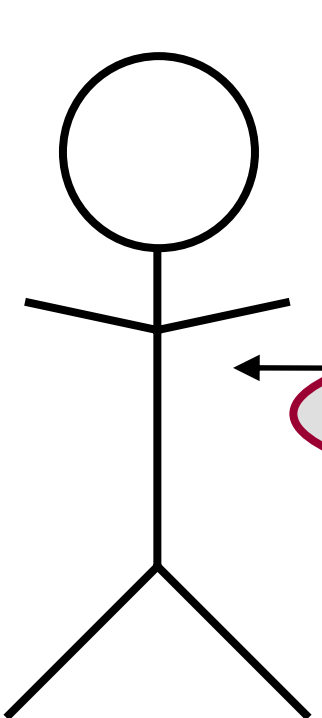


Model for identity management



Model for identity management – anonymity

*



Authorisation



No Identification

Authentication

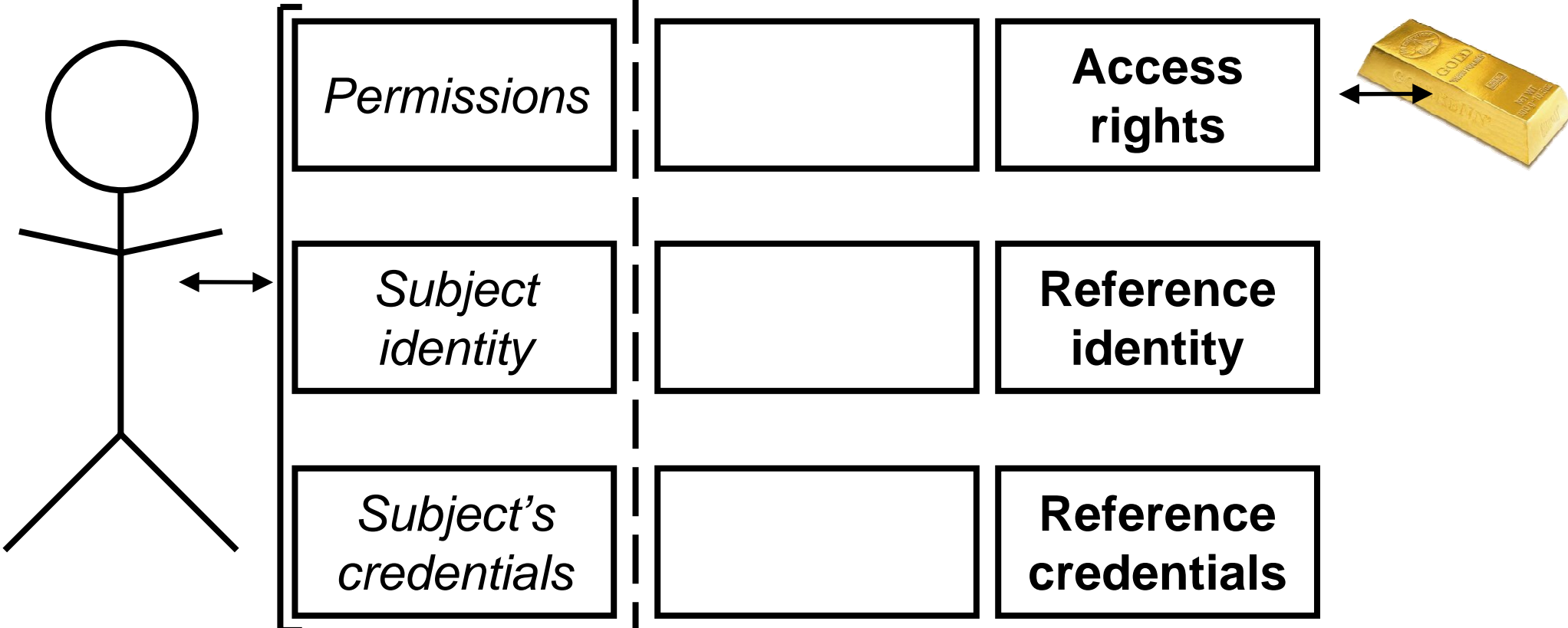
Subject

Claim/
Decision

Reference

Model for identity management – Provisioning

*



Analysis – features of model

- + Holistic approach to identity management
- + Responsibilities, segregation of duties
- + Insourcing, outsourcing, sourcing
- + Architecture – SOA
- + Single customer-view
- + Single sign-on
- + Federation of identities
- + Analysis of decision making process

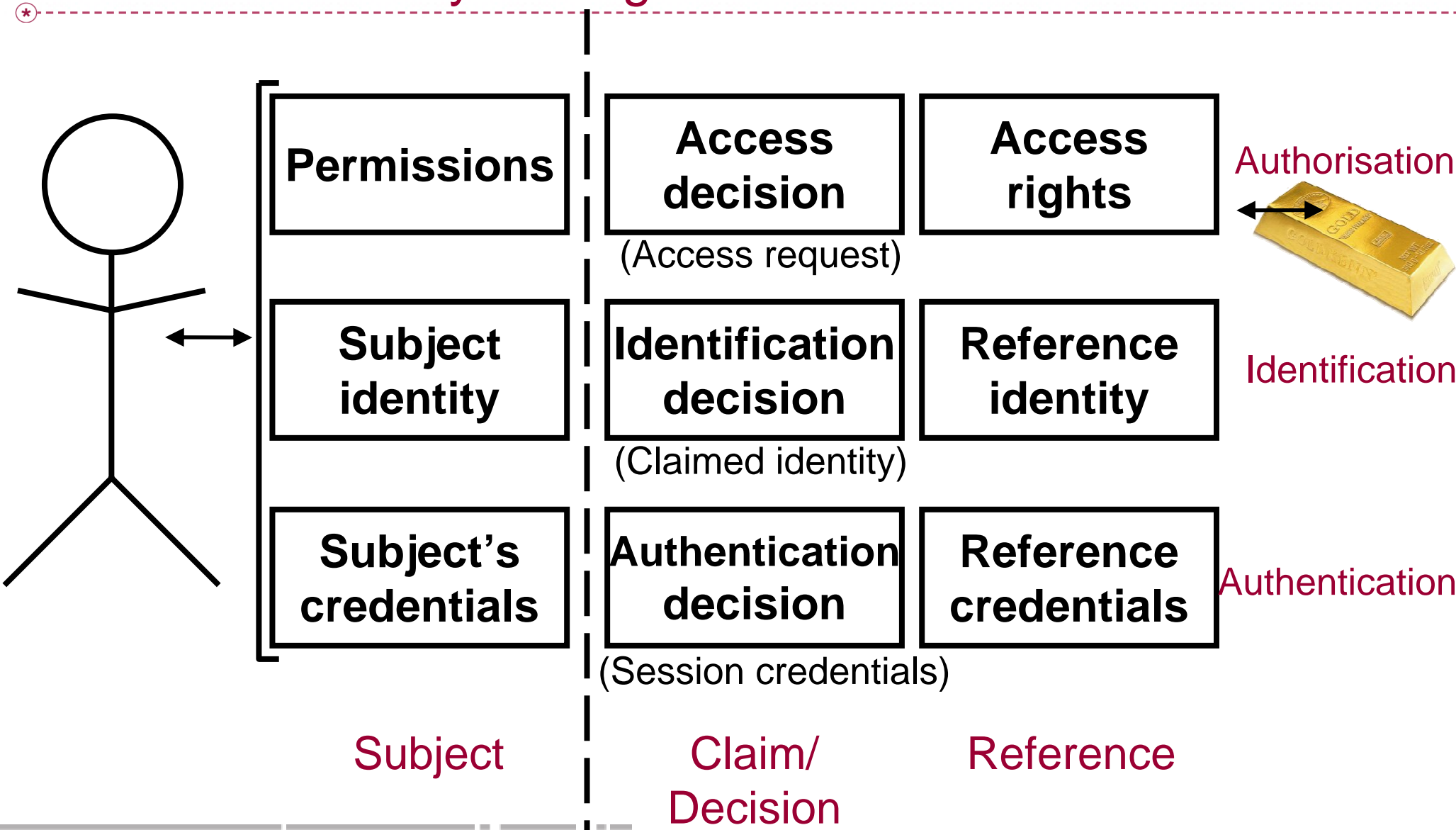
Benefits of identity management model

- + Descriptive and prescriptive
- + Applicable to logical world and physical world
- + Modularity
 - **Vendor independence / subsystem independence**
 - **Basis for outsourcing decisions**
- + Clear distinction authorisation – identification – authentication
 - **Improve auditability**

Limitations to identity management model

- + Does not (explicitly) cover lifecycles
 - **Provisioning, revocation, administration**

Model for identity management



Stephan Overbeek

soverbeek@verisign.com

0431.968.713

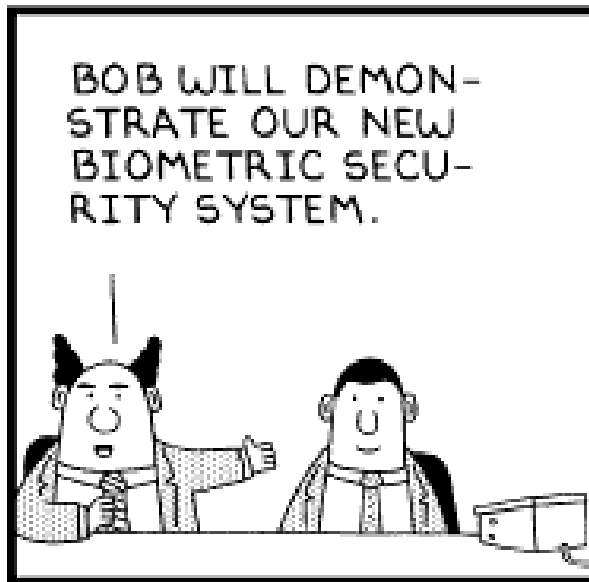
VeriSign

Level 5

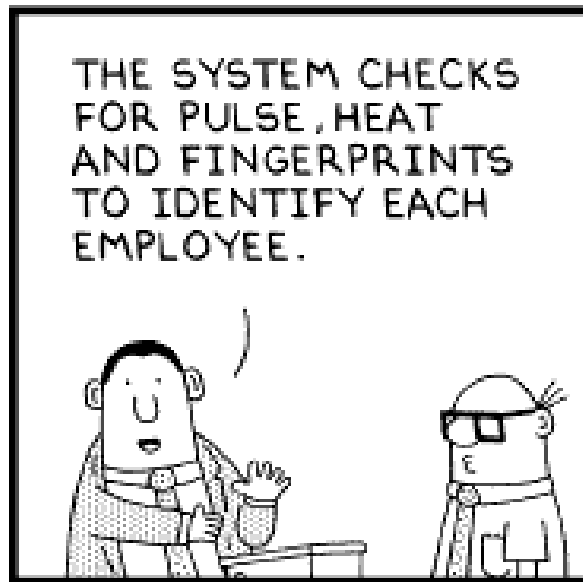
6-10 O'Connell Street

Sydney NSW 2000

02-9236.0509



www.dilbert.com
scottadams@aol.com



12/21/02 © 2002 United Feature Syndicate, Inc.

