Data-centric security in software-defined networks

Dr.-Ing. Konrad Wrona

Lecture 4:
Attibute-based access control

Spectacular failures of data protection and compliance

One slide introduction to data protection

- Confidentiality
  - Controlling who can see

Read

- Integrity
  - Controlling who can change

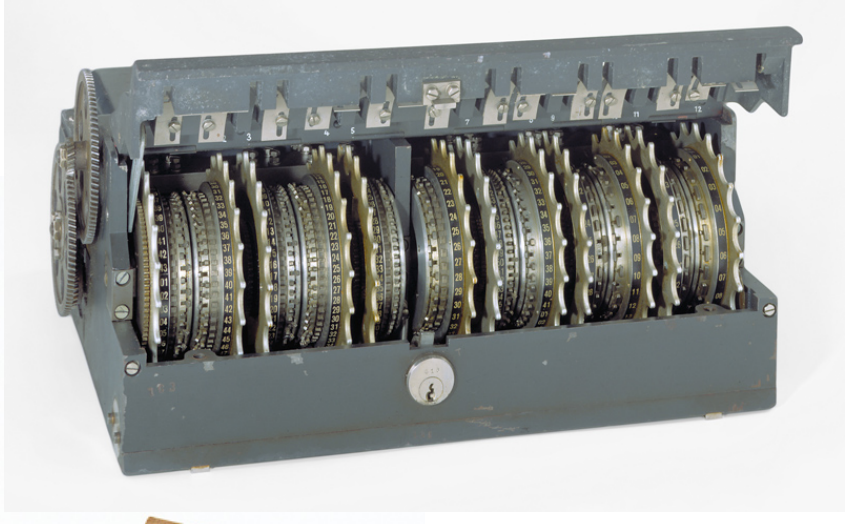
Write

- Availability
  - Controlling who can use

Priority

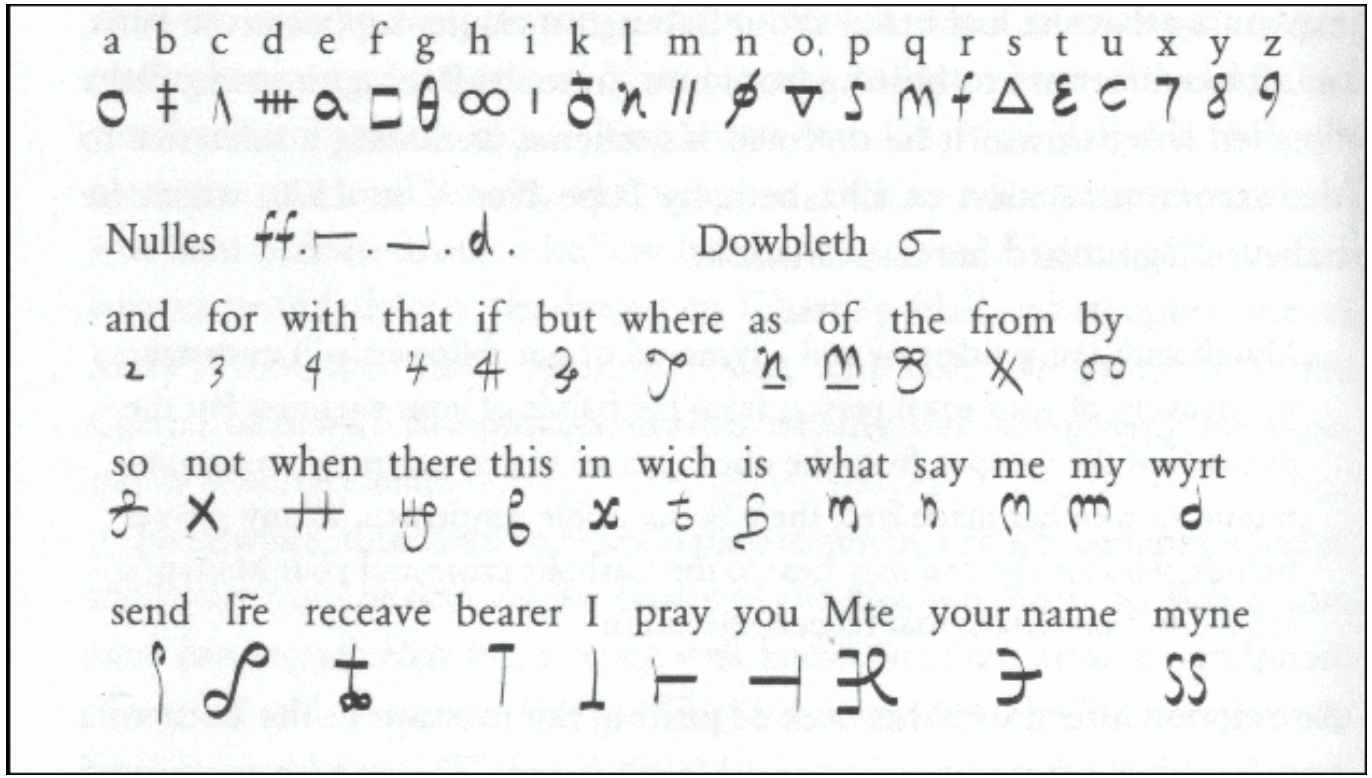
Confidentiality

- Historically main focus for data protection



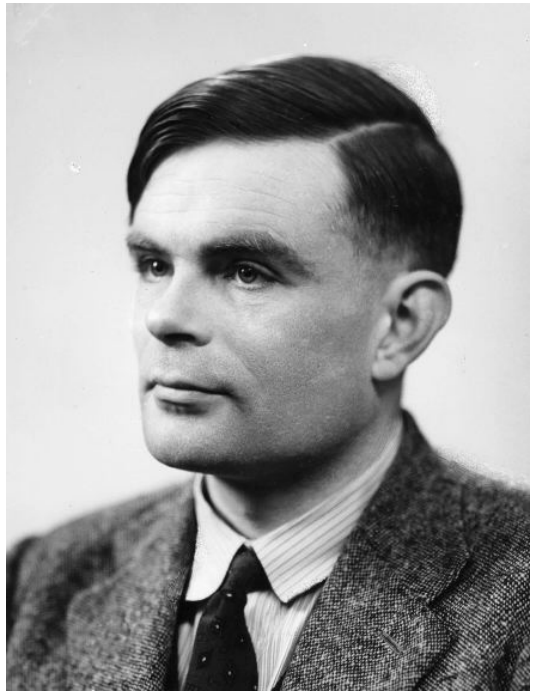
Confidentiality

- Some times it was deciding about life or death



Confidentiality

- Or winning/loosing a war



Integrity and availability is often even more important!

- The best way to protect confidentiality and integrity of information is to make it inaccessible to anybody – but what is the use of it?

Integrity vs trustworthiness

- Technical integrity of information does not guarantee its trustworthiness

ROYAL NAVY

The Board of Admiralty regrets to announce the following casualties which have been sustained in meeting the general hazards of war. Next-of-kin have been notified:—

OFFICERS

KILLED

A/Capt. Sir T. L. Beevor, Bt., R.N.; T/Lt. D. A. Burgass, R.N.V.R.; Lt. J. L. Fraser, R.N.V.R.; Lt. P. F. S. Gould, D.S.C., R.N.; T/Sub-Lt. (A) J. H. Hodgson, R.N.V.R.; T/Spb-Lt. (A) K. R. Joll, R.N.V.R.; Rear-Admiral P. J. Mack, D.S.O.; T/Lt (A) G. Muttrie, R.N.V.R.; T/Lt. (A) G. Raynor, R.N.V.R.; T/Sub-Lt. J. N. Wishart, R.N.V.R.

ROYAL MARINES.—T/Capt (A/Major) W. Martin.

DIED FROM WOUNDS OR INJURIES

T/Sub-Lt. (A) J. Hall, R.N.V.R.; T/Lt. A. G. D. Heybyrne, R.N.V.R.

Integrity can mean many things

Source	Definition
NATO Glossary	The property that information has not been altered or destroyed in an unauthorised manner
UK MOD (unpublished report)	The maintenance of information systems and assets in their complete and proper form [unless correctly amended or deleted by authorized people]
UK HMG IAS 1&2	The property of safeguarding the accuracy and completeness of assets - this may include the ability to prove an action or event has taken place, such that it cannot be repudiated later
ISO 13335-1:2004	The property of safeguarding the accuracy and completeness of assets
44 U.S.C SEC. 3542	The guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity

Integrity

- User
  - trustworthiness of a person
  - the higher the trust in a user, the higher expected integrity of the information created by that user
- System
  - associated with level of system assurance
  - confidence in the system operating as intended can be associated with integrity of produced information

Availability can mean different things, too

Source	Definition
NATO Glossary	The property of information being accessible and usable upon demand by an authorised individual or entity
UK MOD (unpublished report)	The requirement for information to be available by authorized individuals whenever required
FIPS 199	A loss of availability is the disruption of access to or use of information or an information system
ISO/IEC 27000:2014 and UK HMG IAS 1&2	The property of being accessible and usable upon demand by an authorized entity
44 U.S.C SEC. 3542	Ensuring timely and reliable access to and use of information

Availability

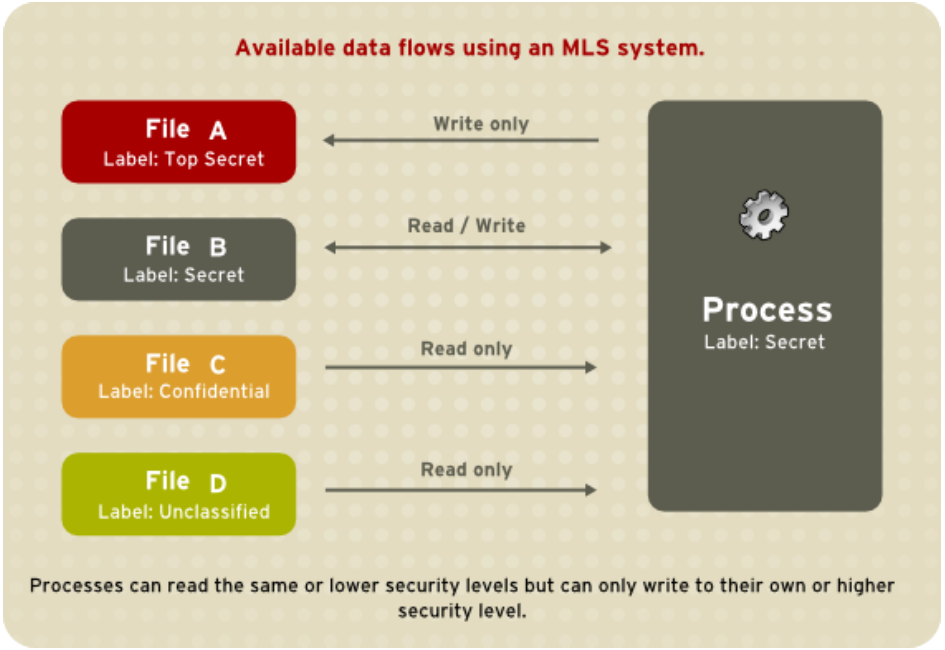
- Interpreted as hosting system availability
  - In respect to both serving and storing the data
  - Users are assumed to be always available
- Availability requirements are expressed in terms of technological constraints, such as bandwidth, storage capacity, power supply, etc.
- Interplay between confidentiality and availability
  - Highest availability channel/storage may offer lowest confidentiality

Correlation between different dimensions

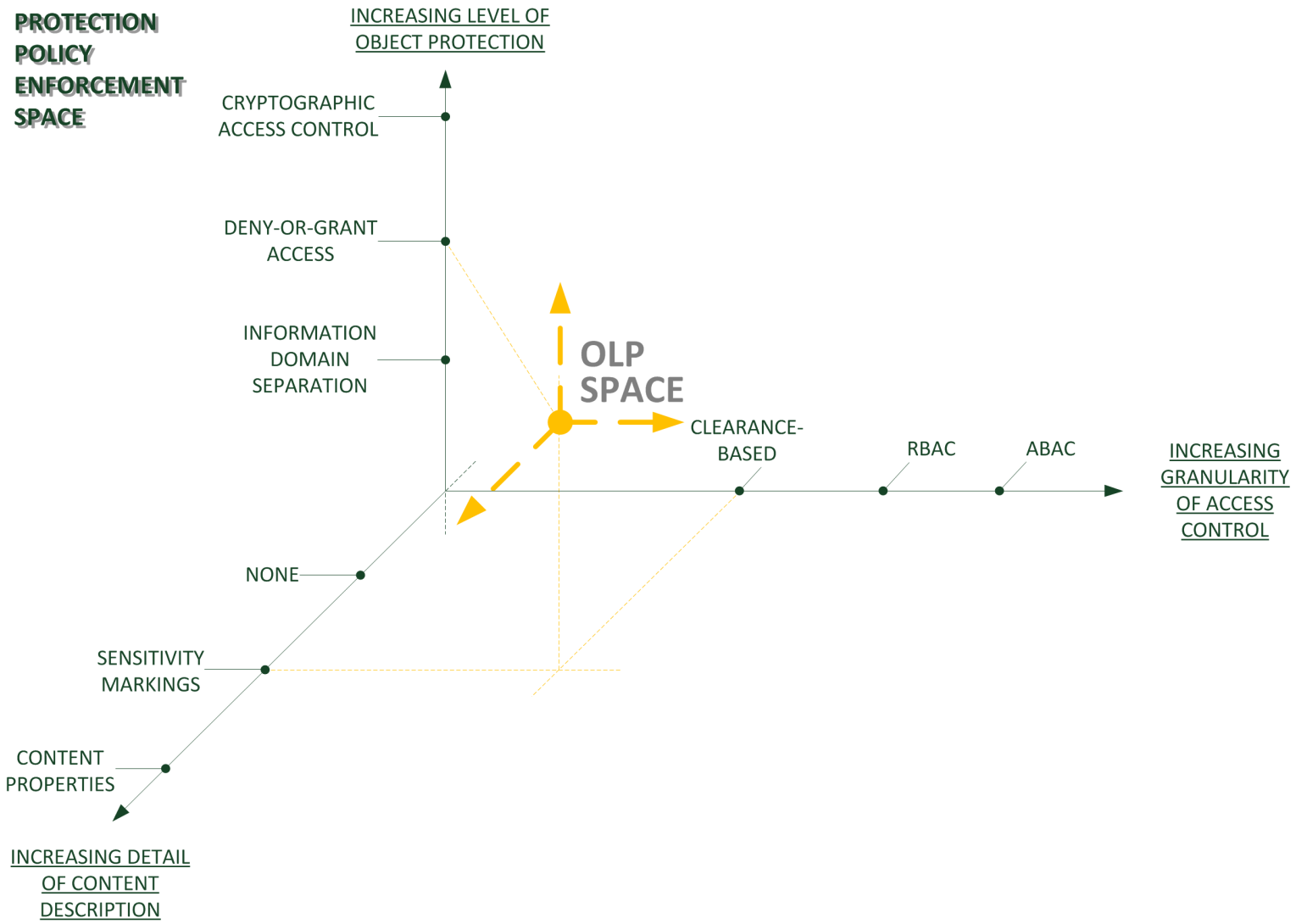
- Intuitively: high confidentiality requirements rather imply high integrity requirements
- Often the same cryptographic measures can be used to provide both confidentiality and integrity protection
  - Public key cryptography, most operational modes of symmetric block ciphers
- But availability and confidentiality are orthogonal – and sometimes in conflict
  - Breaking-glass policies in military and healthcare

Traditional security model: Bell-LaPadula

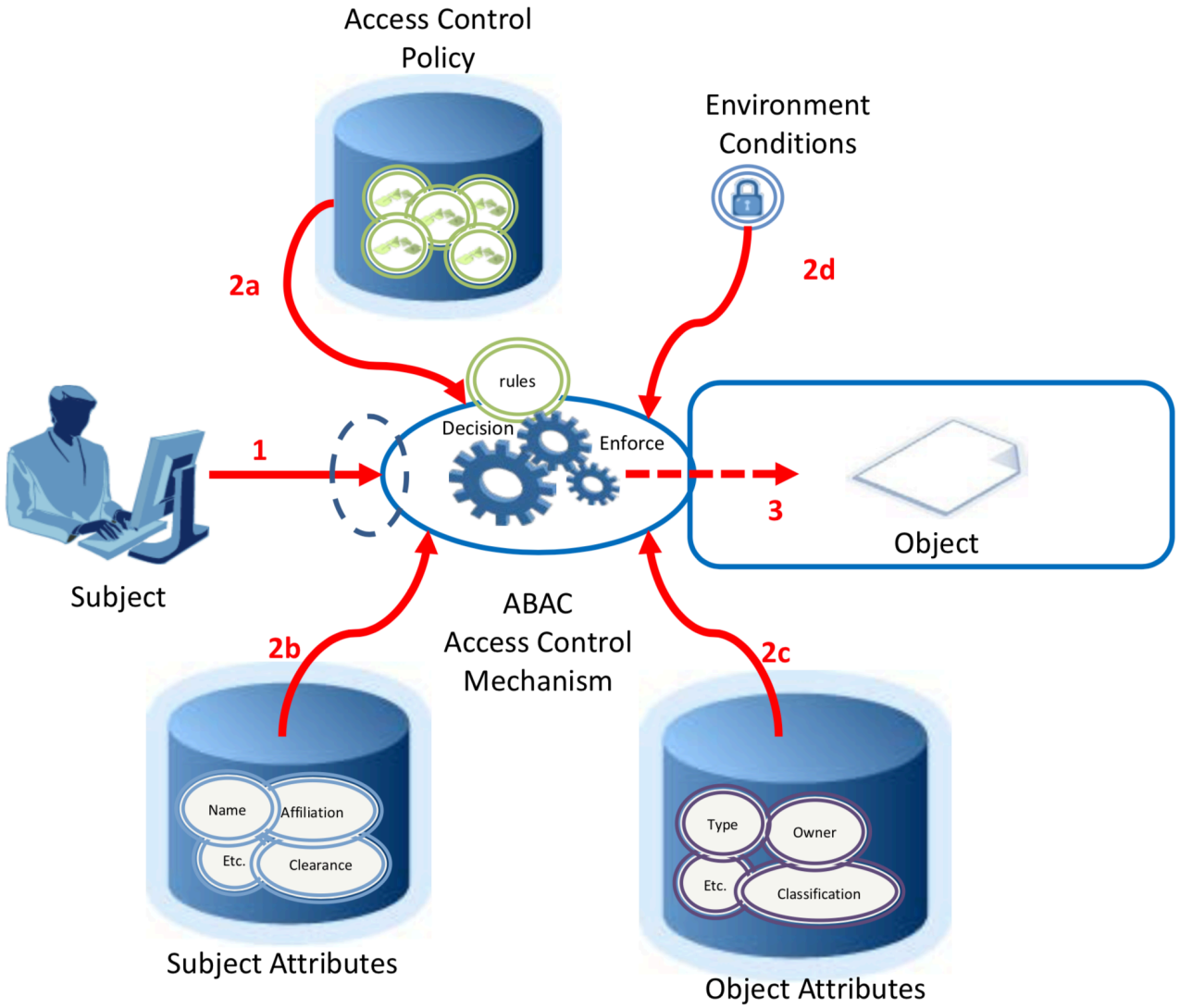
- Simple security property
  - No read up
- * security property
  - No write down
- Tranquility property
  - Strong: Classification of a subject or object can not be modified during system operation
  - Weak: in a way that violates a pre-defined policy



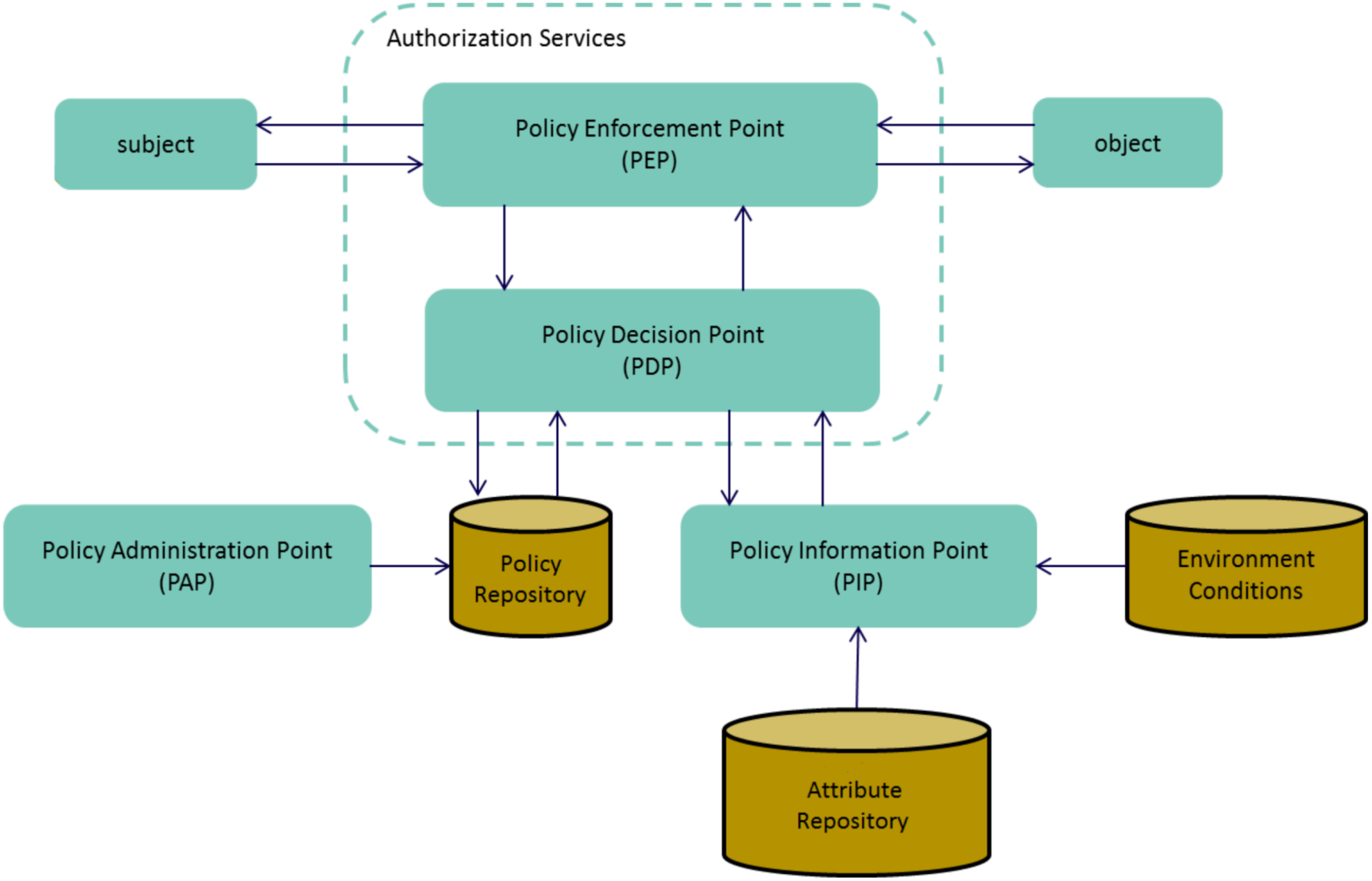
Dimensions of Object Level Protection



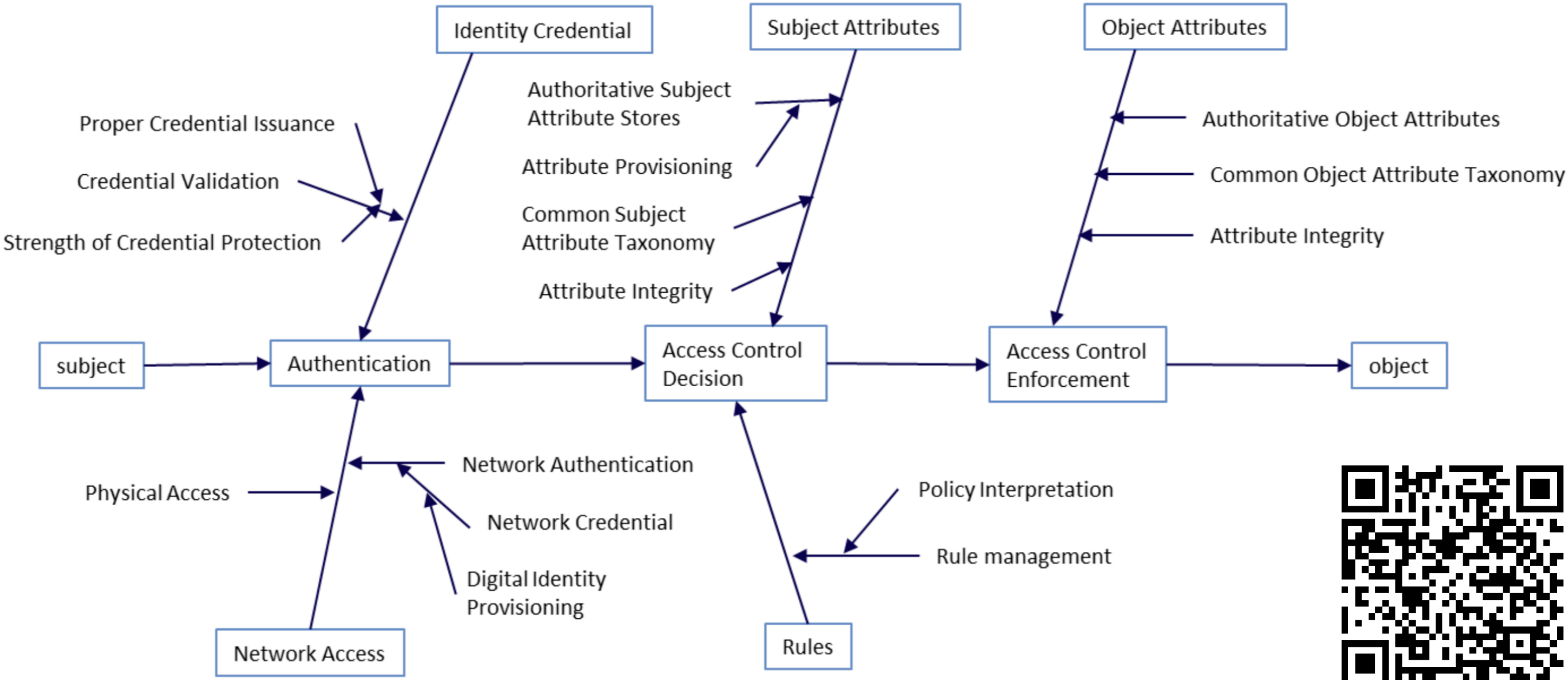
Attribute-base access control model



Attribute-base access control model



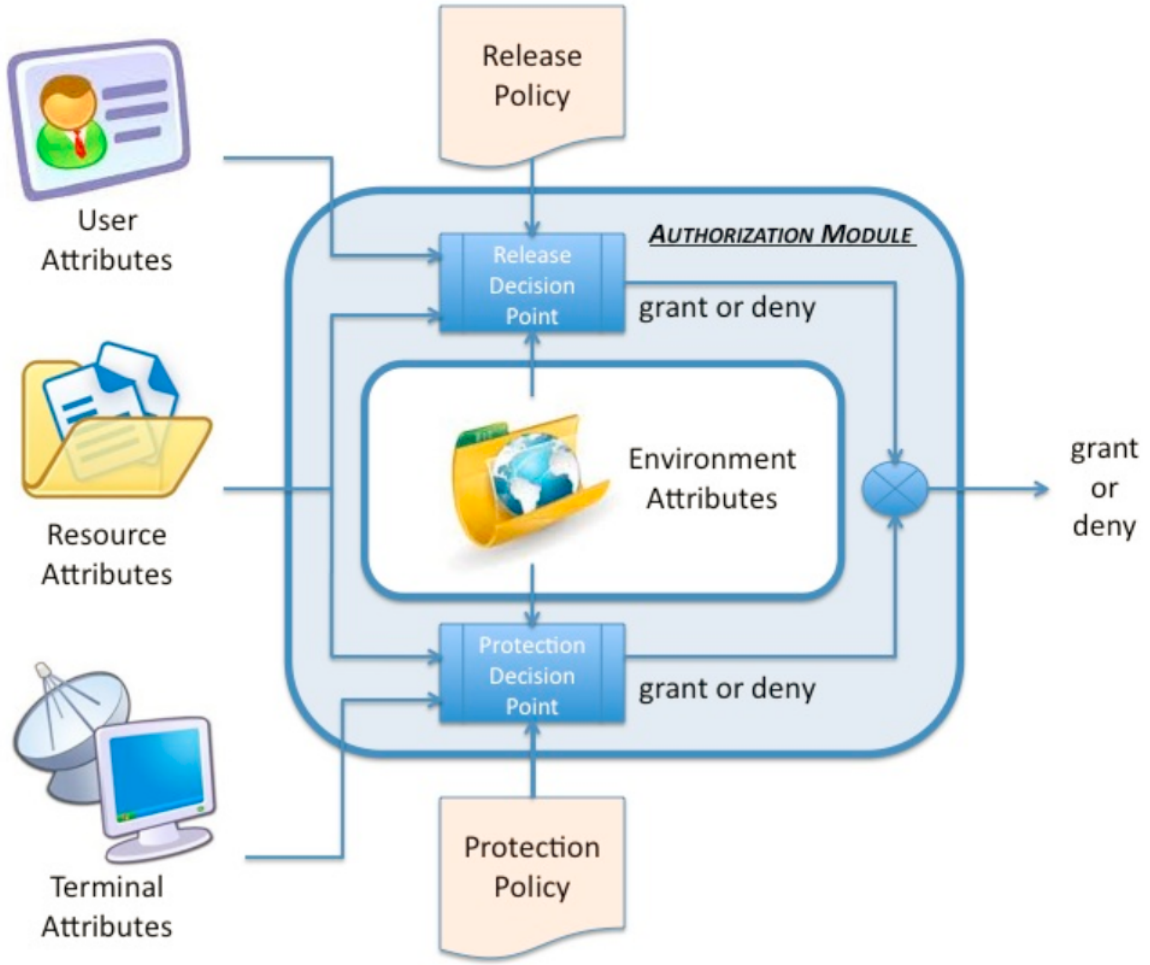
Attribute-base access control model



ABAC for future NATO missions

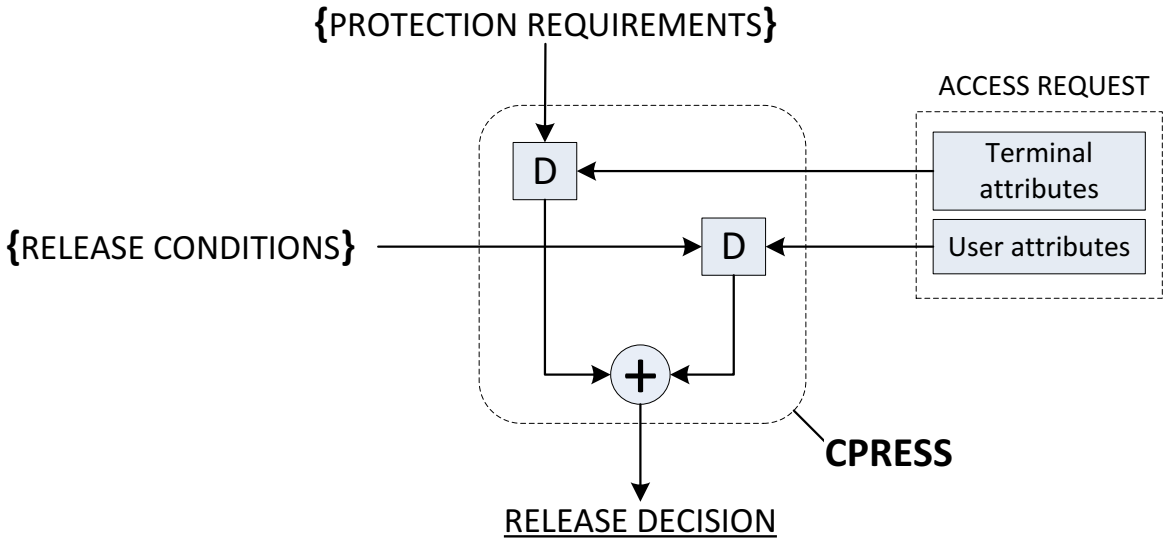
- Timely and secure information sharing in dynamic environment of future NATO missions
- Support changing coalition membership
- Support changing information sharing requirements
- Fulfil responsibility-to-share
- Enforce need-to-know
- See-all-what-you-can on your terminal
- Applicable to single- and cross-domain

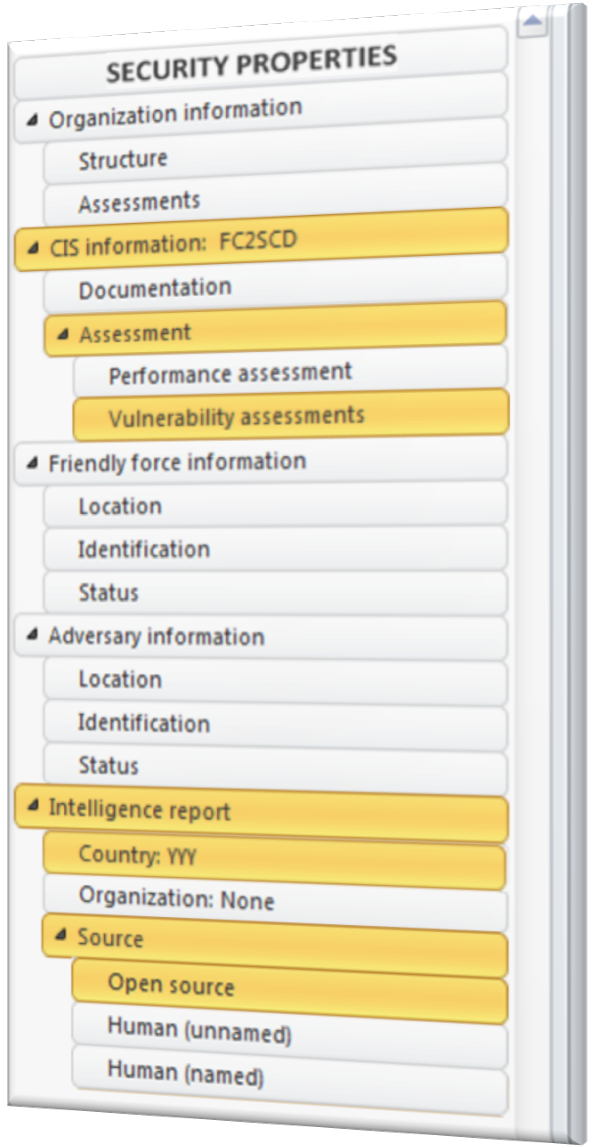
Content-based Protection & Release (CPR)



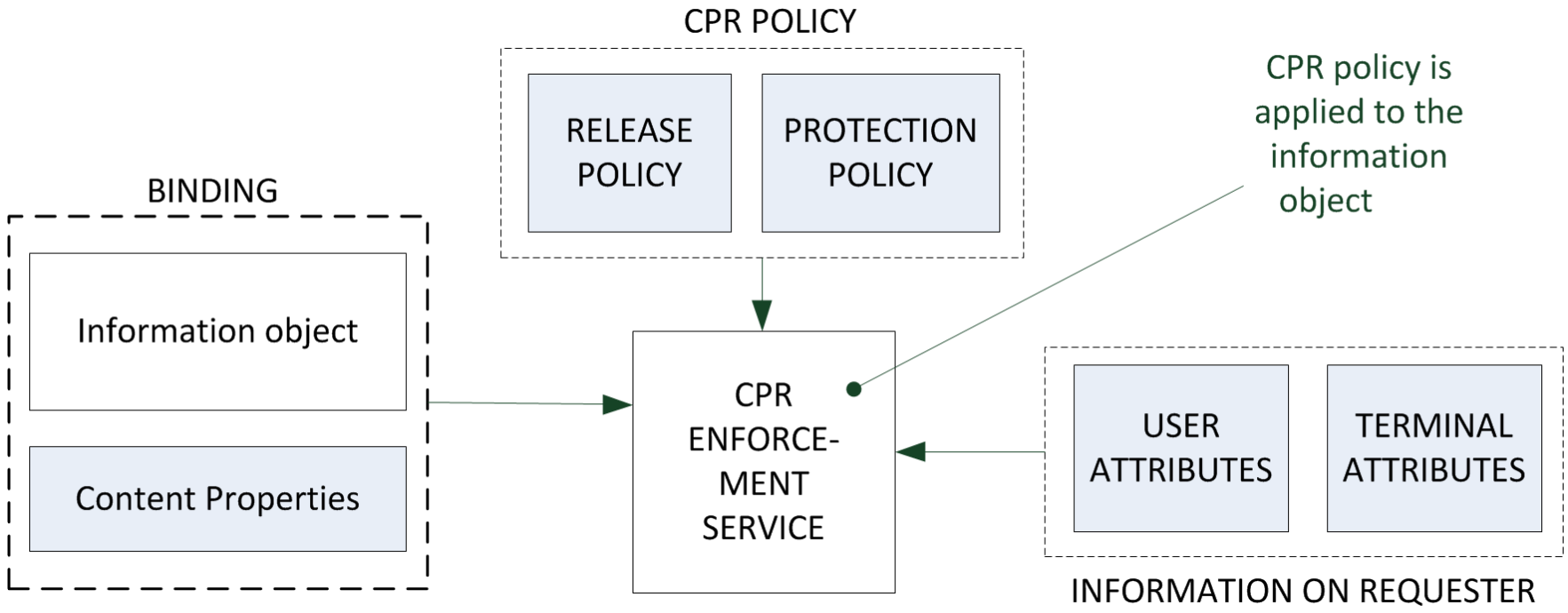
CPR Principles

- Originator defines content description (attributes), not confidentiality markings
- Content attributes determine
  - Protection requirements
    - How the content is to be processed and stored
  - Release conditions
    - To whom it can be released

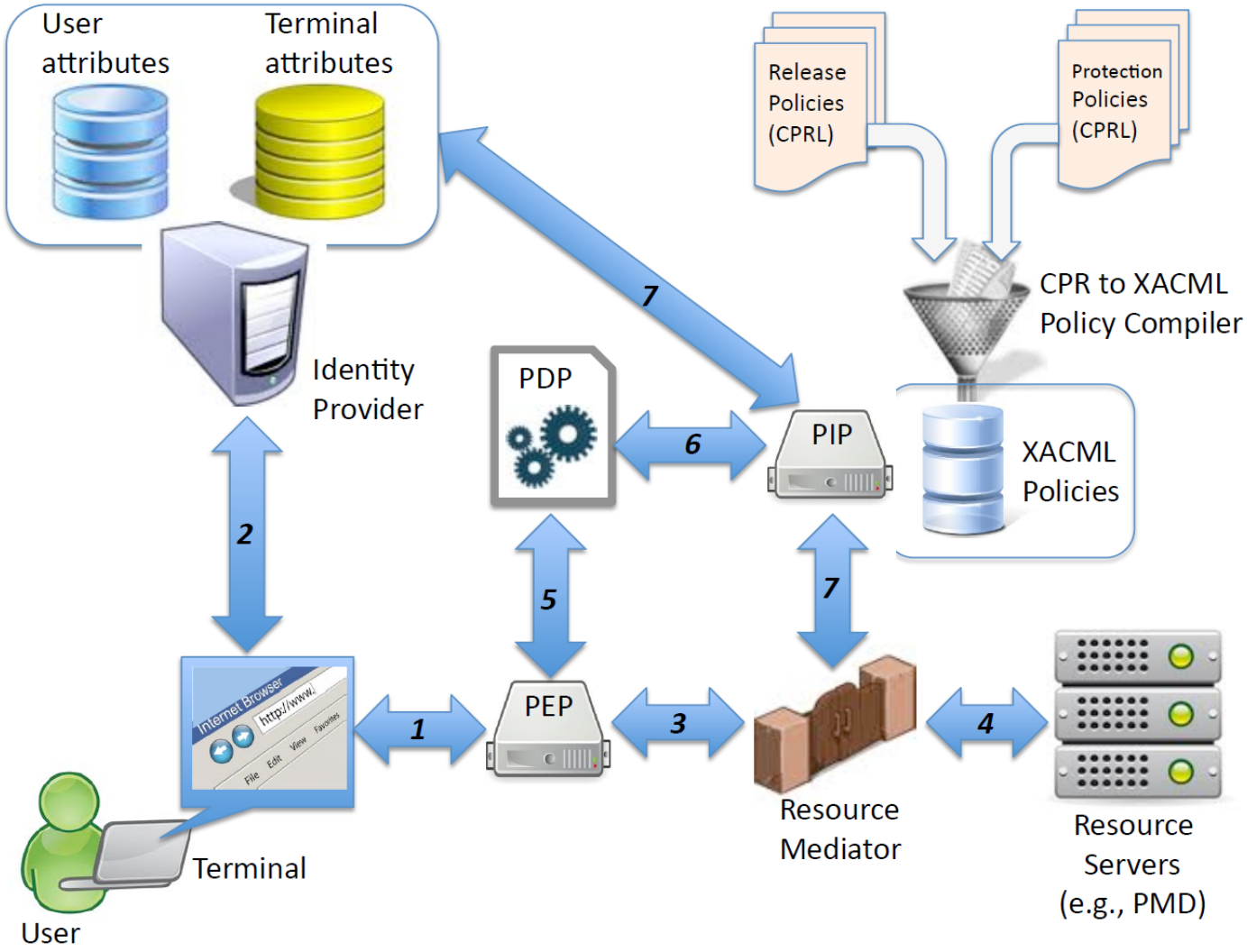




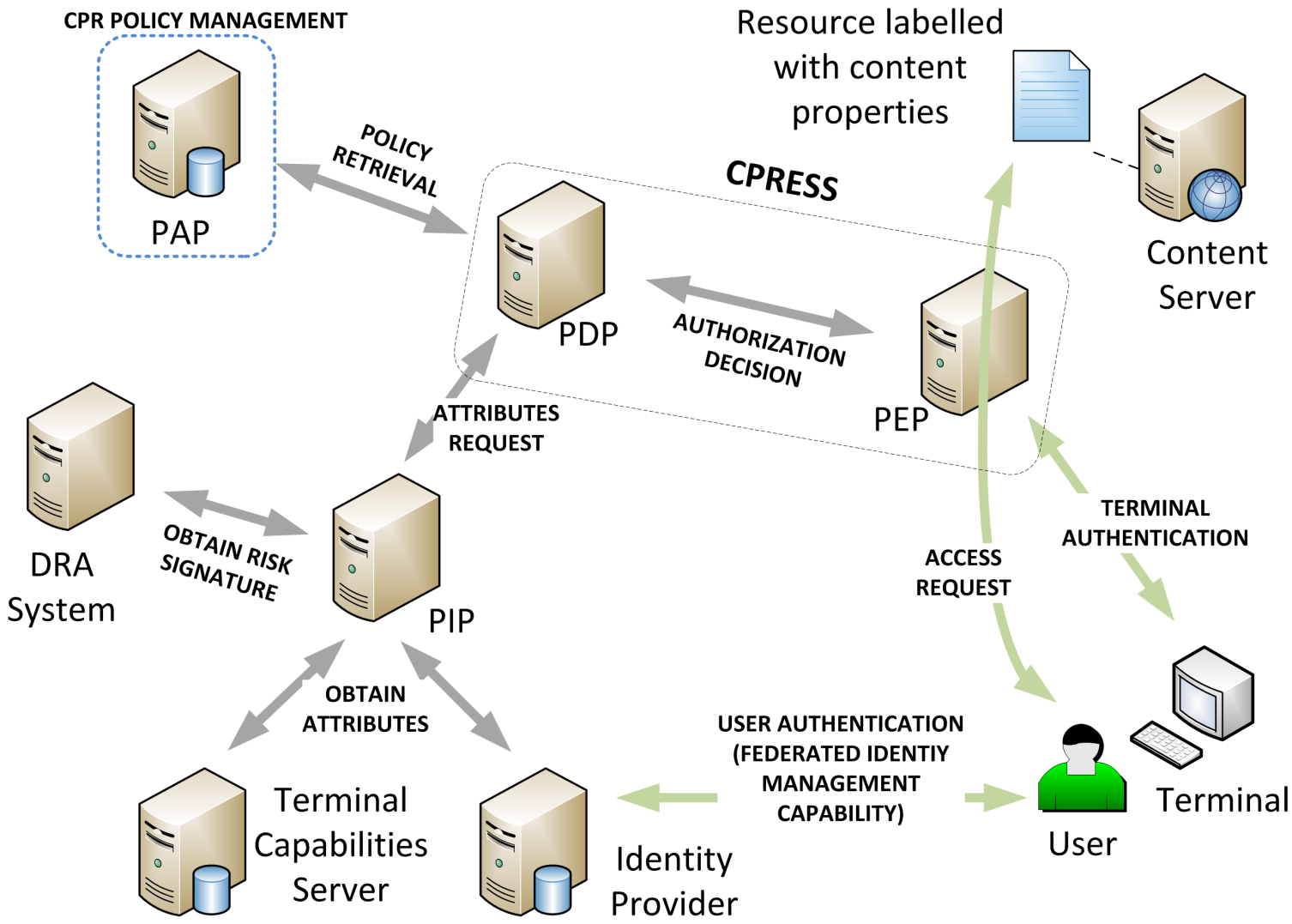
CPR Model


CPR POLICY
RELEASE POLICY
PROTECTION POLICY
CPR policy is applied to the information object
BINDING
Information object
Content Properties
CPR ENFORCE-MENT SERVICE
USER ATTRIBUTES
TERMINAL ATTRIBUTES
INFORMATION ON REQUESTER

Enforcement of CPR



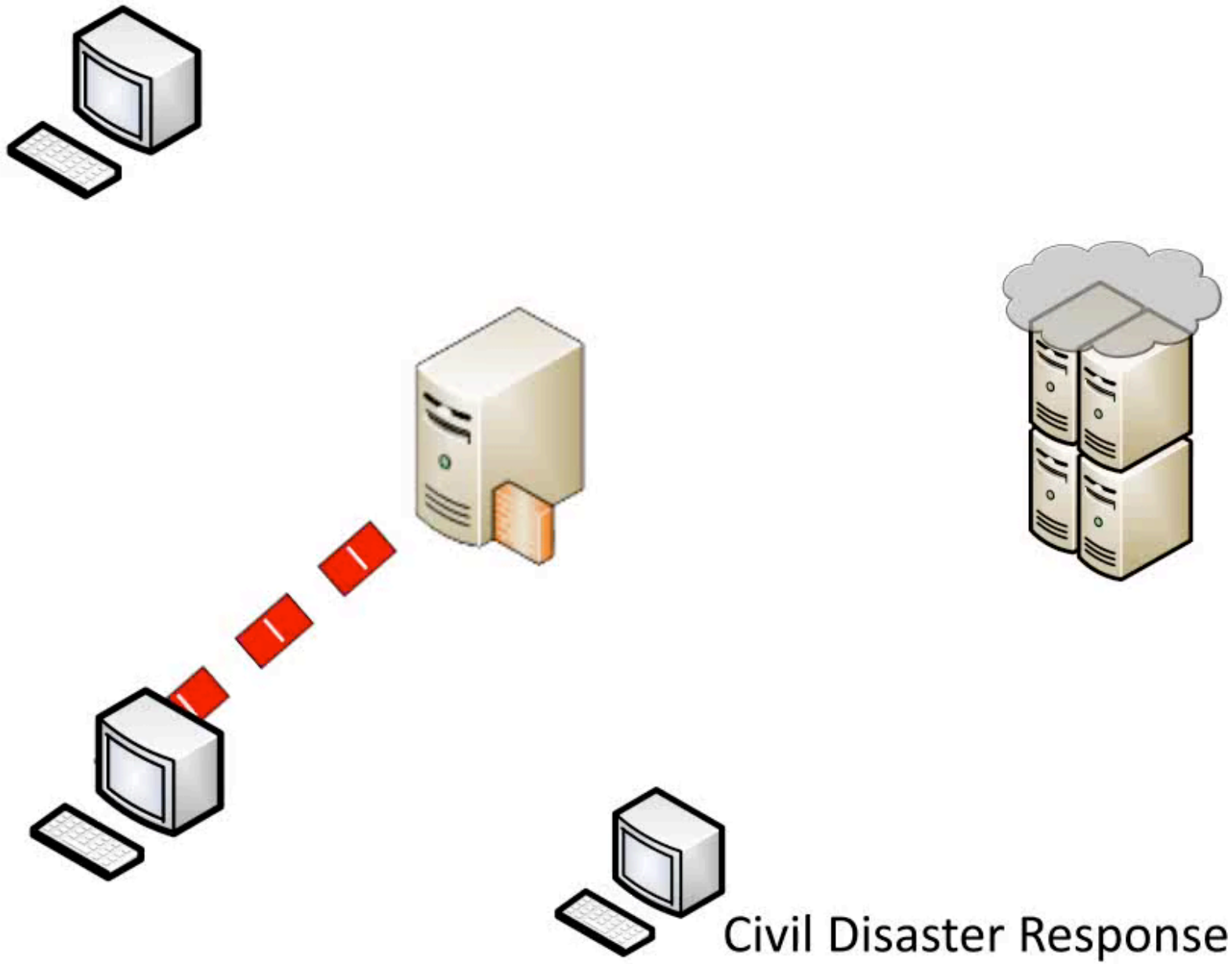
CPR enforcement in XACML architecture



Content-based Protection and Release:

From connecting forces to civil-military interaction

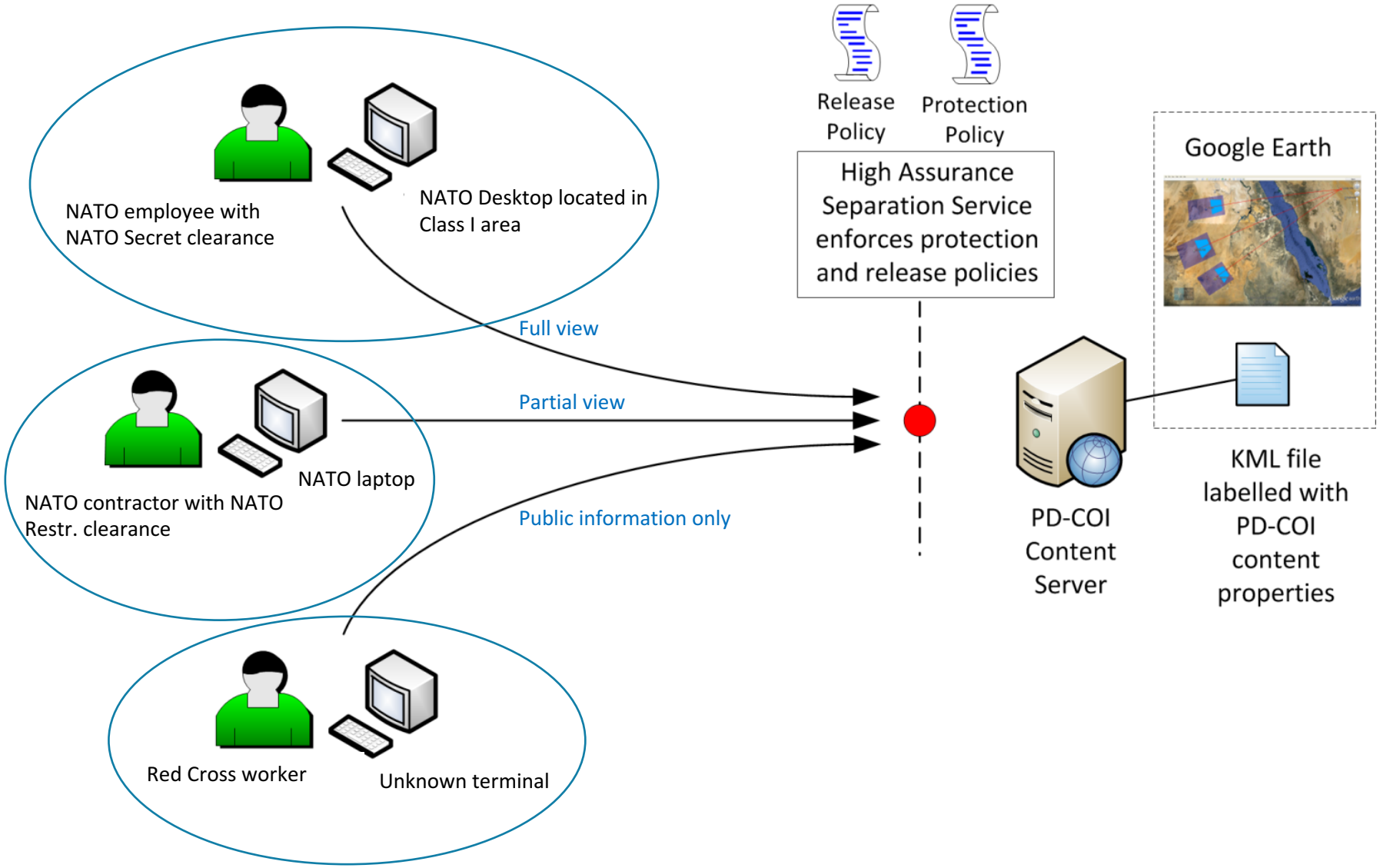
PLANNING



INTEL

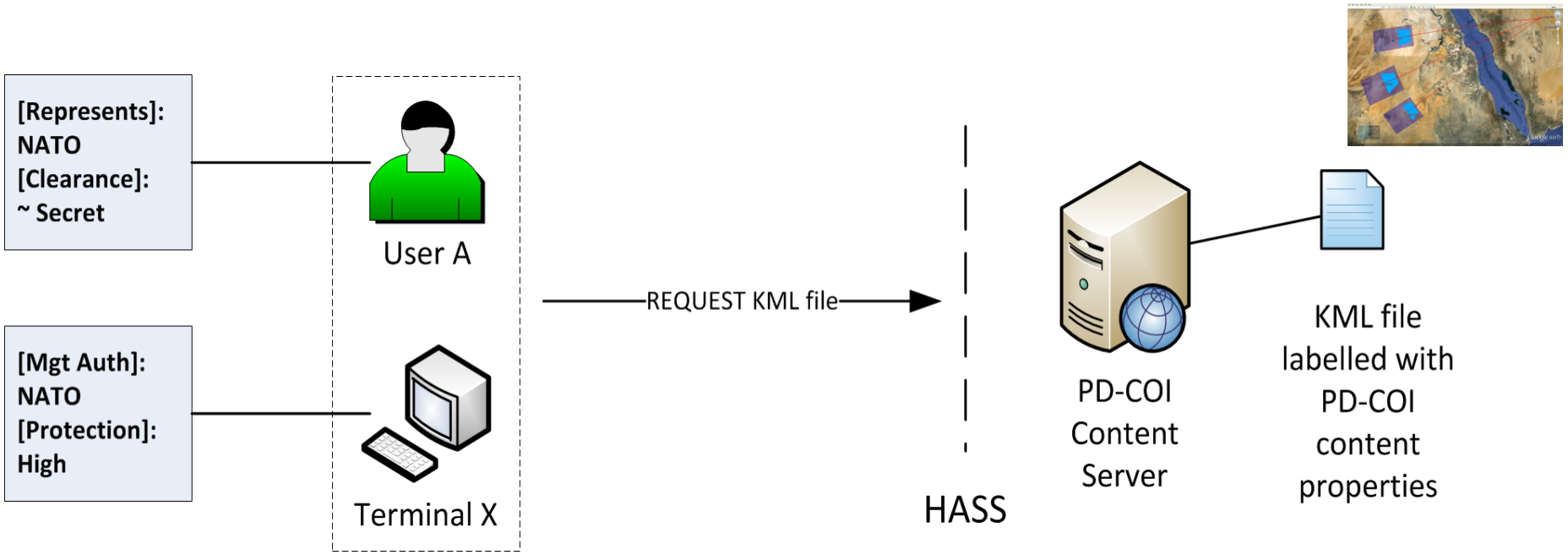
Civil Disaster Response

Information sharing for Passive Missile Defence



Scenario 1

- User A is logged on to Terminal X and requests ‘Operations.kml’



Scenario 1 - Enforcement

Content properties:	User requirements:	Terminal requirements:
Scenario descriptions - Threat operating area	[Represents]: NATO [Clearance]: ~ Secret	[Mgt authority]: NATO [Protection strength]: High
Scenario descriptions - Threat and interceptor trajectory details	[Represents]: NATO [Clearance]: ~ Secret	[Mgt authority]: NATO [Protection strength]: High
Scenario descriptions – High value assets or lists	[Represents]: NATO [Clearance]: ~ Secret	[Mgt authority]: NATO [Protection strength]: High
COI metrics – Sub-munition area location	[Represents]: NATO [Clearance]: ~ Restricted	[Mgt authority]: NATO [Protection strength]: Basic
COI metrics – General hazard area location	[Represents]: NATO [Clearance]: None	[Mgt authority]: NATO [Protection strength]: None
Public information	[Represents]: * (any) [Clearance]: None	[Mgt authority]: * (any) [Protection strength]: None

Scenario 1 - Enforcement

Content properties:	User requirements:	Terminal requirements:
Scenario descriptions - Threat operating area	[Represents]: NATO [Clearance]: ~ Secret	[Mgt authority]: NATO [Protection strength]: High
Scenario descriptions - Threat and interceptor trajectory details	[Represents]: NATO [Clearance]: ~ Secret	[Mgt authority]: NATO [Protection strength]: High
Scenario descriptions – High value assets or lists	[Represents]: NATO [Clearance]: ~ Secret	[Mgt authority]: NATO [Protection strength]: High
COI metrics – Sub-munition area location	[Represents]: NATO [Clearance]: ~ Restricted	[Mgt authority]: NATO [Protection strength]: Basic
COI metrics – General hazard area location	[Represents]: NATO [Clearance]: None	[Mgt authority]: NATO [Protection strength]: None
Public information	[Represents]: * (any) [Clearance]: None	[Mgt authority]: * (any) [Protection strength]: None

User A: NATO person with clearance equivalent to SECRET

Scenario 1 - Enforcement

Content properties:	User requirements:	Terminal requirements:
Scenario descriptions - Threat operating area	[Represents]: NATO [Clearance]: ~ Secret	[Mgt authority]: NATO [Protection strength]: High
Scenario descriptions - Threat and interceptor trajectory details	[Represents]: NATO [Clearance]: ~ Secret	[Mgt authority]: NATO [Protection strength]: High
Scenario descriptions – High value assets or lists	[Represents]: NATO [Clearance]: ~ Secret	[Mgt authority]: NATO [Protection strength]: High
COI metrics – Sub-munition area location	[Represents]: NATO [Clearance]: ~ Restricted	[Mgt authority]: NATO [Protection strength]: Basic
COI metrics – General hazard area location	[Represents]: NATO [Clearance]: None	[Mgt authority]: NATO [Protection strength]: None
Public information	[Represents]: * (any) [Clearance]: None	[Mgt authority]: * (any) [Protection strength]: None

Terminal X: managed by NATO Strength of information protection mechanisms: high

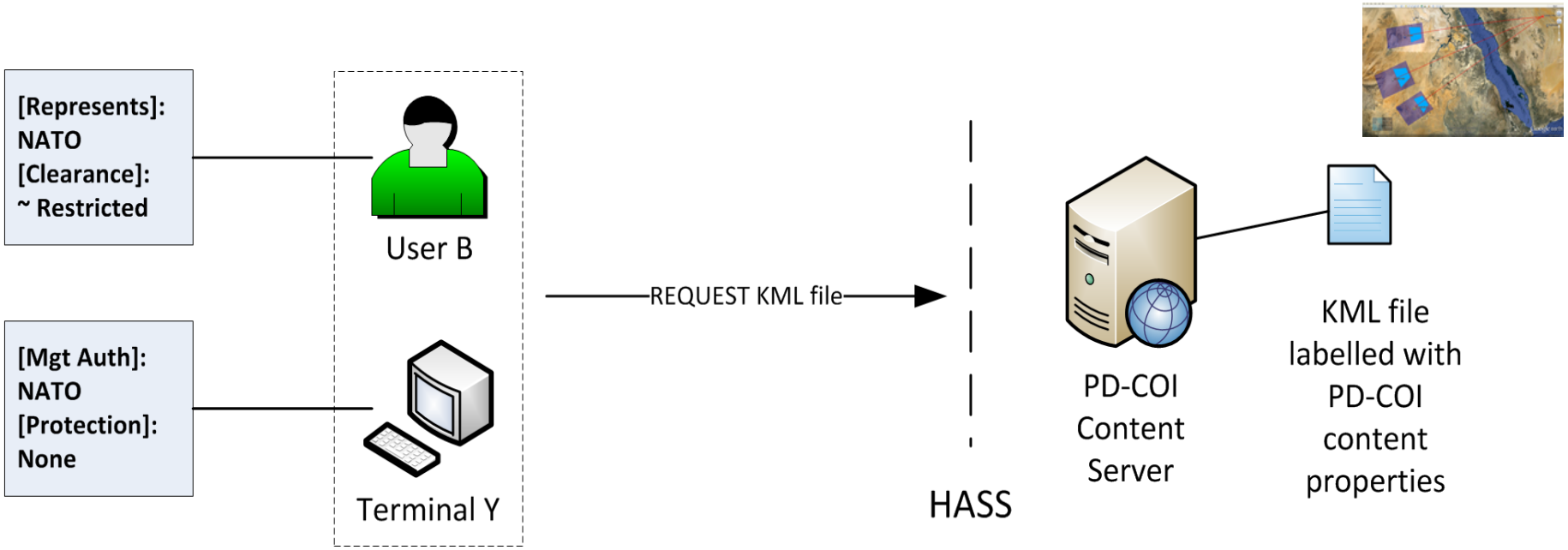
Scenario 1 - Enforcement

Content properties:	User requirements:	Terminal requirements:
Scenario descriptions - Threat operating area	[Represents]: NATO [Clearance]: ~ Secret	[Mgt authority]: NATO [Protection strength]: High
Scenario descriptions - Threat and interceptor trajectory details	[Represents]: NATO [Clearance]: ~ Secret	[Mgt authority]: NATO [Protection strength]: High
Scenario descriptions – High value assets or lists	[Represents]: NATO [Clearance]: ~ Secret	[Mgt authority]: NATO [Protection strength]: High
COI metrics – Sub-munition area location	[Represents]: NATO [Clearance]: ~ Restricted	[Mgt authority]: NATO [Protection strength]: Basic
COI metrics – General hazard area location	[Represents]: NATO [Clearance]: None	[Mgt authority]: NATO [Protection strength]: None
Public information	[Represents]: * (any) [Clearance]: None	[Mgt authority]: * (any) [Protection strength]: None

The view presented to User A at Terminal X contains all placemarks in 'Operations.kml'

Scenario 2

- User B is logged on to Terminal Y and requests ‘Operations.kml’



Scenarion 2 - Enforcement

Content properties:	User requirements:	Terminal requirements:
Scenario descriptions - Threat operating area	[Represents]: NATO [Clearance]: ~ Secret	[Mgt authority]: NATO [Protection strength]: High
Scenario descriptions - Threat and interceptor trajectory details	[Represents]: NATO [Clearance]: ~ Secret	[Mgt authority]: NATO [Protection strength]: High
Scenario descriptions – High value assets or lists	[Represents]: NATO [Clearance]: ~ Secret	[Mgt authority]: NATO [Protection strength]: High
COI metrics – Sub-munition area location	[Represents]: NATO [Clearance]: ~ Restricted	[Mgt authority]: NATO [Protection strength]: Basic
COI metrics – General hazard area location	[Represents]: NATO [Clearance]: None	[Mgt authority]: NATO [Protection strength]: None
Public information	[Represents]: * (any) [Clearance]: None	[Mgt authority]: * (any) [Protection strength]: None

Scenarion 2 - Enforcement

Content properties:	User requirements:	Terminal requirements:
	[Represents]: NATO [Clearance]: ~ Secret	[Mgt authority]: NATO [Protection strength]: High
	[Represents]: NATO [Clearance]: ~ Secret	[Mgt authority]: NATO [Protection strength]: High
	[Represents]: NATO [Clearance]: ~ Secret	[Mgt authority]: NATO [Protection strength]: High
COI metrics – Sub-munition area location	[Represents]: NATO [Clearance]: ~ Restricted	[Mgt authority]: NATO [Protection strength]: Basic
COI metrics – General hazard area location	[Represents]: NATO [Clearance]: None	[Mgt authority]: NATO [Protection strength]: None
Public information	[Represents]: * (any) [Clearance]: None	[Mgt authority]: * (any) [Protection strength]: None

User B:
NATO personnel with clearance equivalent to RESTRICTED

Scenarion 2 - Enforcement

Content properties:	User requirements:	Terminal requirements:
	[Represents]: NATO [Clearance]: ~ Secret	[Mgt authority]: NATO [Protection strength]: High
	[Represents]: NATO [Clearance]: ~ Secret	[Mgt authority]: NATO [Protection strength]: High
	[Represents]: NATO [Clearance]: ~ Secret	[Mgt authority]: NATO [Protection strength]: High
	[Represents]: NATO [Clearance]: ~ Restricted	[Mgt authority]: NATO [Protection strength]: Basic
COI metrics – General hazard area location	[Represents]: NATO [Clearance]: None	[Mgt authority]: NATO [Protection strength]: None
Public information	[Represents]: * (any) [Clearance]: None	[Mgt authority]: * (any) [Protection strength]: None

Terminal Y: managed by NATO, Strength of information protection mechanisms: none

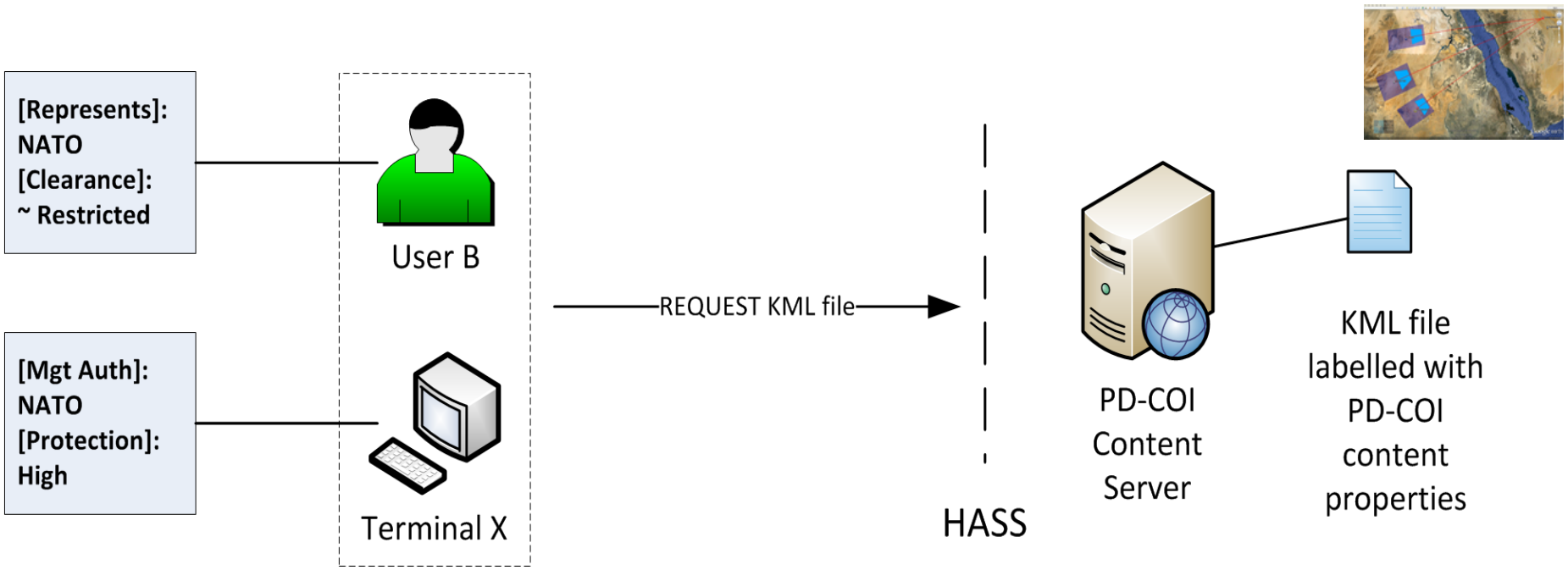
Scenarion 2 - Enforcement

Content properties:	User requirements:	Terminal requirements:
	[Represents]: NATO [Clearance]: ~ Secret	[Mgt authority]: NATO [Protection strength]: High
	[Represents]: NATO [Clearance]: ~ Secret	[Mgt authority]: NATO [Protection strength]: High
	[Represents]: NATO [Clearance]: ~ Secret	[Mgt authority]: NATO [Protection strength]: High
	[Represents]: NATO [Clearance]: ~ Restricted	[Mgt authority]: NATO [Protection strength]: Basic
COI metrics – General hazard area location	[Represents]: NATO [Clearance]: None	[Mgt authority]: NATO [Protection strength]: None
Public information	[Represents]: * (any) [Clearance]: None	[Mgt authority]: * (any) [Protection strength]: None

The view presented to User B at Terminal Y contains a subset of all placemarks in Operations.kml

Scenario 3

- User B is now logged on to Terminal X and requests ‘Operations.kml’



Scenario 3 - Enforcement

Content properties:	User requirements:	Terminal requirements:
Scenario descriptions - Threat operating area	[Represents]: NATO [Clearance]: ~ Secret	[Mgt authority]: NATO [Protection strength]: High
Scenario descriptions - Threat and interceptor trajectory details	[Represents]: NATO [Clearance]: ~ Secret	[Mgt authority]: NATO [Protection strength]: High
Scenario descriptions – High value assets or lists	[Represents]: NATO [Clearance]: ~ Secret	[Mgt authority]: NATO [Protection strength]: High
COI metrics – Sub-munition area location	[Represents]: NATO [Clearance]: ~ Restricted	[Mgt authority]: NATO [Protection strength]: Basic
COI metrics – General hazard area location	[Represents]: NATO [Clearance]: None	[Mgt authority]: NATO [Protection strength]: None
Public information	[Represents]: * (any) [Clearance]: None	[Mgt authority]: * (any) [Protection strength]: None

Scenario 3 - Enforcement

Content properties:	User requirements:	Terminal requirements:
Scenario descriptions - Threat operating area	[Represents]: NATO [Clearance]: ~ Secret	[Mgt authority]: NATO [Protection strength]: High
Scenario descriptions - Threat and interceptor trajectory details	[Represents]: NATO [Clearance]: ~ Secret	[Mgt authority]: NATO [Protection strength]: High
Scenario descriptions – High value assets or lists	[Represents]: NATO [Clearance]: ~ Secret	[Mgt authority]: NATO [Protection strength]: High
COI metrics – Sub-munition area location	[Represents]: NATO [Clearance]: ~ Restricted	[Mgt authority]: NATO [Protection strength]: Basic
COI metrics – General hazard area location	[Represents]: NATO [Clearance]: None	[Mgt authority]: NATO [Protection strength]: None
Public information	[Represents]: * (any) [Clearance]: None	[Mgt authority]: * (any) [Protection strength]: None

Terminal X: managed by NATO

Strength of information protection mechanisms: high

Scenario 3 - Enforcement

Content properties:	User requirements:	Terminal requirements:
	[Represents]: NATO [Clearance]: ~ Secret	[Mgt authority]: NATO [Protection strength]: High
	[Represents]: NATO [Clearance]: ~ Secret	[Mgt authority]: NATO [Protection strength]: High
	[Represents]: NATO [Clearance]: ~ Secret	[Mgt authority]: NATO [Protection strength]: High
COI metrics – Sub-munition area location	[Represents]: NATO [Clearance]: ~ Restricted	[Mgt authority]: NATO [Protection strength]: Basic
COI metrics – General hazard area location	[Represents]: NATO [Clearance]: None	[Mgt authority]: NATO [Protection strength]: None
Public information	[Represents]: * (any) [Clearance]: None	[Mgt authority]: * (any) [Protection strength]: None

User B:
NATO personnel with clearance equivalent to RESTRICTED

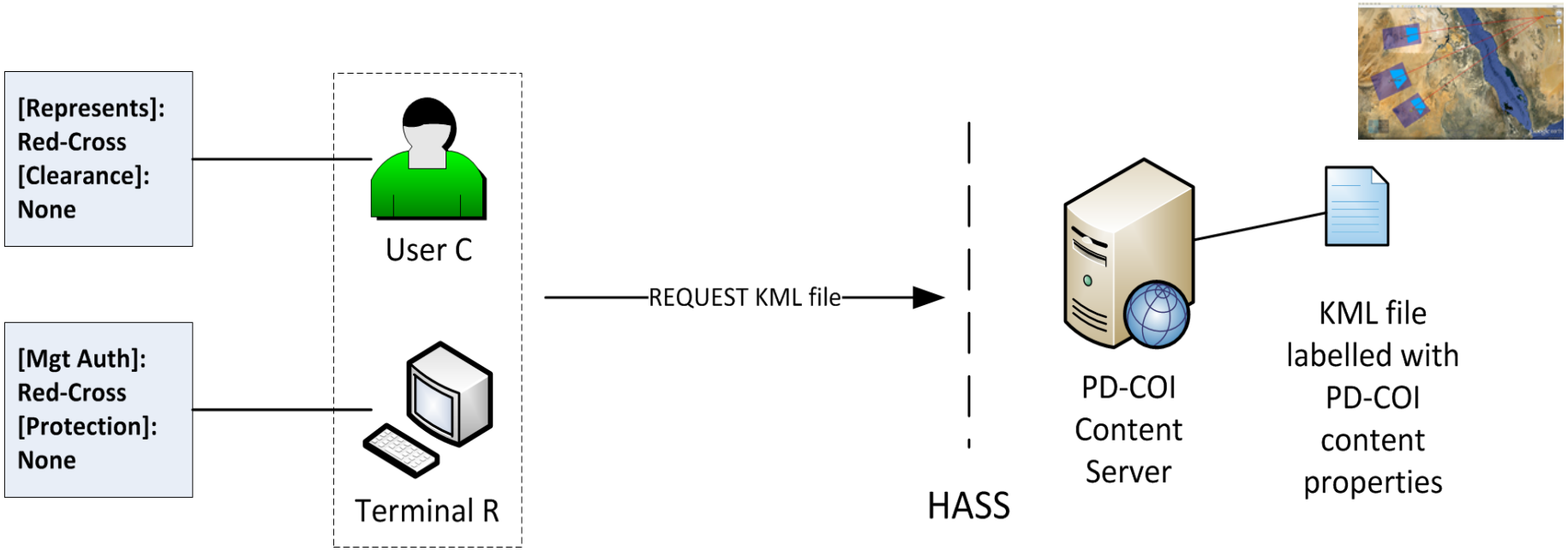
Scenario 3 - Enforcement

Content properties:	User requirements:	Terminal requirements:
	[Represents]: NATO [Clearance]: ~ Secret	[Mgt authority]: NATO [Protection strength]: High
	[Represents]: NATO [Clearance]: ~ Secret	[Mgt authority]: NATO [Protection strength]: High
	[Represents]: NATO [Clearance]: ~ Secret	[Mgt authority]: NATO [Protection strength]: High
COI metrics – Sub-munition area location	[Represents]: NATO [Clearance]: ~ Restricted	[Mgt authority]: NATO [Protection strength]: Basic
COI metrics – General hazard area location	[Represents]: NATO [Clearance]: None	[Mgt authority]: NATO [Protection strength]: None
Public information	[Represents]: * (any) [Clearance]: None	[Mgt authority]: * (any) [Protection strength]: None

The view presented to User B at Terminal X contains a subset of placemarks in Operations.kml

Scenario 4

- User C is logged on to Terminal R and requests ‘Operations.kml’



Scenario 4 - Enforcement

Content properties:	User requirements:	Terminal requirements:
Scenario descriptions - Threat operating area	[Represents]: NATO [Clearance]: ~ Secret	[Mgt authority]: NATO [Protection strength]: High
Scenario descriptions - Threat and interceptor trajectory details	[Represents]: NATO [Clearance]: ~ Secret	[Mgt authority]: NATO [Protection strength]: High
Scenario descriptions – High value assets or lists	[Represents]: NATO [Clearance]: ~ Secret	[Mgt authority]: NATO [Protection strength]: High
COI metrics – Sub-munition area location	[Represents]: NATO [Clearance]: ~ Restricted	[Mgt authority]: NATO [Protection strength]: Basic
COI metrics – General hazard area location	[Represents]: NATO [Clearance]: None	[Mgt authority]: NATO [Protection strength]: None
Public information	[Represents]: * (any) [Clearance]: None	[Mgt authority]: * (any) [Protection strength]: None

Scenario 4 - Enforcement

Content properties:	User requirements:	Terminal requirements:
	[Represents]: NATO [Clearance]: ~ Secret	[Mgt authority]: NATO [Protection strength]: High
	[Represents]: NATO [Clearance]: ~ Secret	[Mgt authority]: NATO [Protection strength]: High
	[Represents]: NATO [Clearance]: ~ Secret	[Mgt authority]: NATO [Protection strength]: High
	[Represents]: NATO [Clearance]: ~ Restricted	[Mgt authority]: NATO [Protection strength]: Basic
	[Represents]: NATO [Clearance]: None	[Mgt authority]: NATO [Protection strength]: None
Public information	[Represents]: * (any) [Clearance]: None	[Mgt authority]: * (any) [Protection strength]: None

User C
Red Cross representative with no clearance

Scenario 4 - Enforcement

Content properties:	User requirements:	Terminal requirements:
	[Represents]: NATO [Clearance]: ~ Secret	[Mgt authority]: NATO [Protection strength]: High
	[Represents]: NATO [Clearance]: ~ Secret	[Mgt authority]: NATO [Protection strength]: High
	[Represents]: NATO [Clearance]: ~ Secret	[Mgt authority]: NATO [Protection strength]: High
	[Represents]: NATO [Clearance]: ~ Restricted	[Mgt authority]: NATO [Protection strength]: Basic
	[Represents]: NATO [Clearance]: None	[Mgt authority]: NATO [Protection strength]: None
Public information	[Represents]: * (any) [Clearance]: None	[Mgt authority]: * (any) [Protection strength]: None

Terminal R: managed by Red-Cross, Strength of information protection mechanisms: none

Scenario 4 - Enforcement

Content properties:	User requirements:	Terminal requirements:
	[Represents]: NATO [Clearance]: ~ Secret	[Mgt authority]: NATO [Protection strength]: High
	[Represents]: NATO [Clearance]: ~ Secret	[Mgt authority]: NATO [Protection strength]: High
	[Represents]: NATO [Clearance]: ~ Secret	[Mgt authority]: NATO [Protection strength]: High
	[Represents]: NATO [Clearance]: ~ Restricted	[Mgt authority]: NATO [Protection strength]: Basic
	[Represents]: NATO [Clearance]: None	[Mgt authority]: NATO [Protection strength]: None
Public information	[Represents]: * (any) [Clearance]: None	[Mgt authority]: * (any) [Protection strength]: None

The view presented to User C at Terminal R contains only those placemarks in 'Operations.kml' that have the property 'Public Information'

Scenario 5

- The CPR protection and release policy are updated to reflect the decision that placemarks with content property “General hazard area location” can now be shared with Red Cross users (on Red Cross terminals)

Content properties:	User requirements:	Terminal requirements:
COI metrics – General hazard area location	[Represents]: NATO <OR> **Red-Cross** [Clearance]: None	[Mgt authority]: NATO <OR> **Red-Cross** [Protection strength]: None

- The view presented to User C at Terminal R contains placemarks with the property ‘Public information’ or ‘Ground hazard area location

Example of release policy for Smart Engagement and Monitoring (SEM)

				USERS					
Property	**Value**	**Pseudocode**	**User restriction**	U_1	U_2	U_3	U_4	U_5	U_6
originatingNetwork	**Link16**	Pass if clearance is secret	(user.clearance = Secret)	PASS	PASS	PASS	STOP	STOP	STOP
	Others	Pass	n.a.	PASS	PASS	PASS	PASS	PASS	PASS

CPR: Release policy for SEM

			USERS					
Property	**Value**	**User restriction**	U_1	U_2	U_3	U_4	U_5	U_6
identity	**Hostile**	(user.department = A2) & (user_with_NATO_member_nation) & (user.clearance = Secret)	STOP	STOP	PASS	STOP	STOP	STOP
	Others	(((user.department = A2) | (user.department = A5)) & (user_with_NATO_member_nation) & ((user.clearance = Restricted) | (user.clearance = Confidential) | (user.clearance = Secret))) | ((resource.age > 1 day) & ((user_with_NATO_member_nation) | (user.organization = NGO)))	STOP	STOP	PASS	if old enough	STOP	PASS

CPR: Release policy for SEM

			USERS					
Property	**Value**	**User restriction**	U_1	U_2	U_3	U_4	U_5	U_6
originatingMission	M_ORANGE	user.missionMembership = M_ORANGE | user_with_NATO_member_nation	STOP	PASS	PASS	PASS	STOP	PASS
	Null	(user_with_NATO_member_nation)	STOP	STOP	PASS	STOP	STOP	PASS
velocity and heading	at least one exists	n.a	PASS	PASS	PASS	PASS	PASS	PASS
	neither exists	n.a	PASS	PASS	PASS	PASS	PASS	PASS
originatingEntity	SEW	(user.organization = NATO) | (user.organization = NGO) | (user_with_NATO_member_nation)	STOP	STOP	PASS	PASS	STOP	PASS
	Others	((user.organization = NATO) | (user_with_NATO_member_nation)) & ((user.clearance = Restricted) | (user.clearance = Confidential) | (user.clearance = Secret))	STOP	STOP	PASS	STOP	STOP	PASS

CPR: Protection policy for SEM

				Terminals					
Property	**Value**	**Pseudocode**	**Terminal restriction**	T_1	T_2	T_3	T_4	T_5	T_6
originatingNetwork	**Link16**	Pass if terminal is of high confidentiality and from NATO or NATO member nation	(terminal_with_NATO | terminal_with_NATO_member_nation) & (terminal.confidentiality = High)	PASS	STOP	PASS	STOP	STOP	STOP

Ensuring policy consistency with formal modelling and automated validation

- Formal model for CPR policies based on first-order many-sorted logic
  - u can execute a on r in e under ρ, α_U, α_A, α_R, and α_E iff

$$\alpha_U(u) \wedge \alpha_A(a) \wedge \alpha_R(r) \wedge \alpha_E(e) \wedge \rho(u, a, r, e)$$

    is satisfiable modulo T_{CPR} (i.e. there exists a model of T_{CPR} and a variable assignment to the variables in the formula such that the formula holds in the model under the variable assignment), and

  - a can be executed on r via t in e under π, α_A, α_R, α_T, and α_E iff

$$\alpha_A(a) \wedge \alpha_R(r) \wedge \alpha_T(t) \wedge \alpha_E(e) \wedge \pi(a, r, t, e)$$

    is satisfiable modulo T_{CPR}.

Ensuring policy consistency with formal modelling and automated validation

- Formal model for CPR policies based on first-order many-sorted logic
- CPR language for validation of policies

```
(define (rel_1 u::Users r::Resources e::Environments)::bool
(and (= (select u U@from) NATO) (he_Sec u)
     (= (select r R@cat) Descr) (or (= (select r R@top) Toas)
                                    (= (select r R@top) TItds))))
(define (rel_2 u::Users r::Resources e::Environments)::bool
(and (= (select u U@from) NATO) (he_Res u)
     (= (select r R@cat) MCOI)  (= (select r R@top) Smal)))
(define (rel_3 u::Users r::Resources e::Environments)::bool
(and (= (select u U@from) NATO) (he_Pub u)
     (= (select r R@cat) MCOI)  (= (select r R@top) Hal)))
(define (rel_4 u::Users r::Resources e::Environments)::bool
(and (he_Pub u) (= (select r R@cat) PI)))
```

Ensuring policy consistency with formal modelling and automated validation

- Formal model for CPR policies based on first-order many-sorted logic
- CPR language for validation of policies
- User-friendly specification language

```
release pmd_6 =
 clr_he_PUBLIC &
 (resource.category = PUBLIC_INFORMATION) ;
protection pmd_2 =
    (resource.category = SCENARIO_DESCRIPTIONS) &
    (resource.topic = THREAT_AND_INTERCEPTOR_TRAJECTORY_DETAILS) &
    (resource.mission = MISSION_POSSIBLE) &
    (terminal.authority = NATO) ;
```

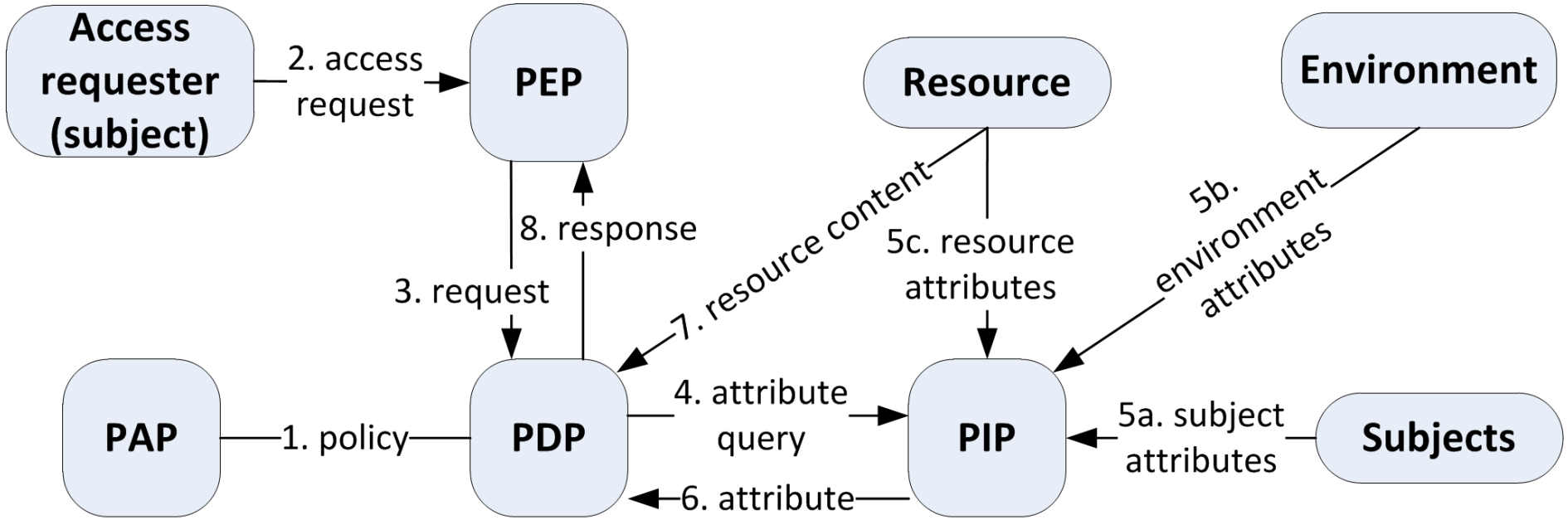
Ensuring policy consistency with formal modelling and automated validation

- Formal model for CPR policies based on first-order many-sorted logic
- CPR language for validation of policies
- User-friendly specification language
- Automated translation of CPR policies into XACML

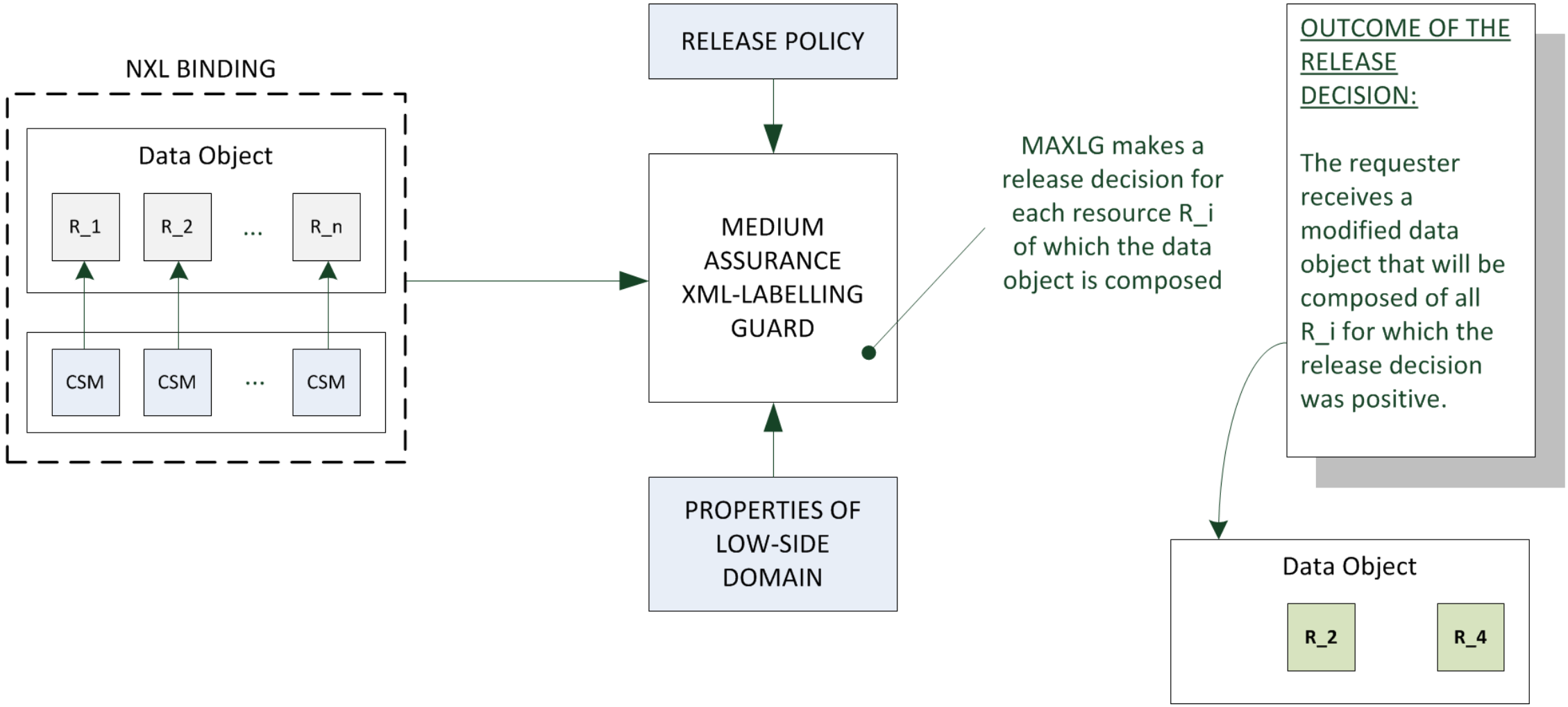
```
Policy -
<Environments>
  <Environment>
   <EnvironmentMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
equal">
    <AttributeValue DataType="http://www.w3.org/2001/
XMLSchema#string">wso2.domain</AttributeValue>

    <EnvironmentAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:environment:envi
ronment-id" DataType="http://www.w3.org/2001/
XMLSchema#string"/>
   </EnvironmentMatch>
  </Environment>
</Environments>
```

Two approaches to access control: Authorization-based

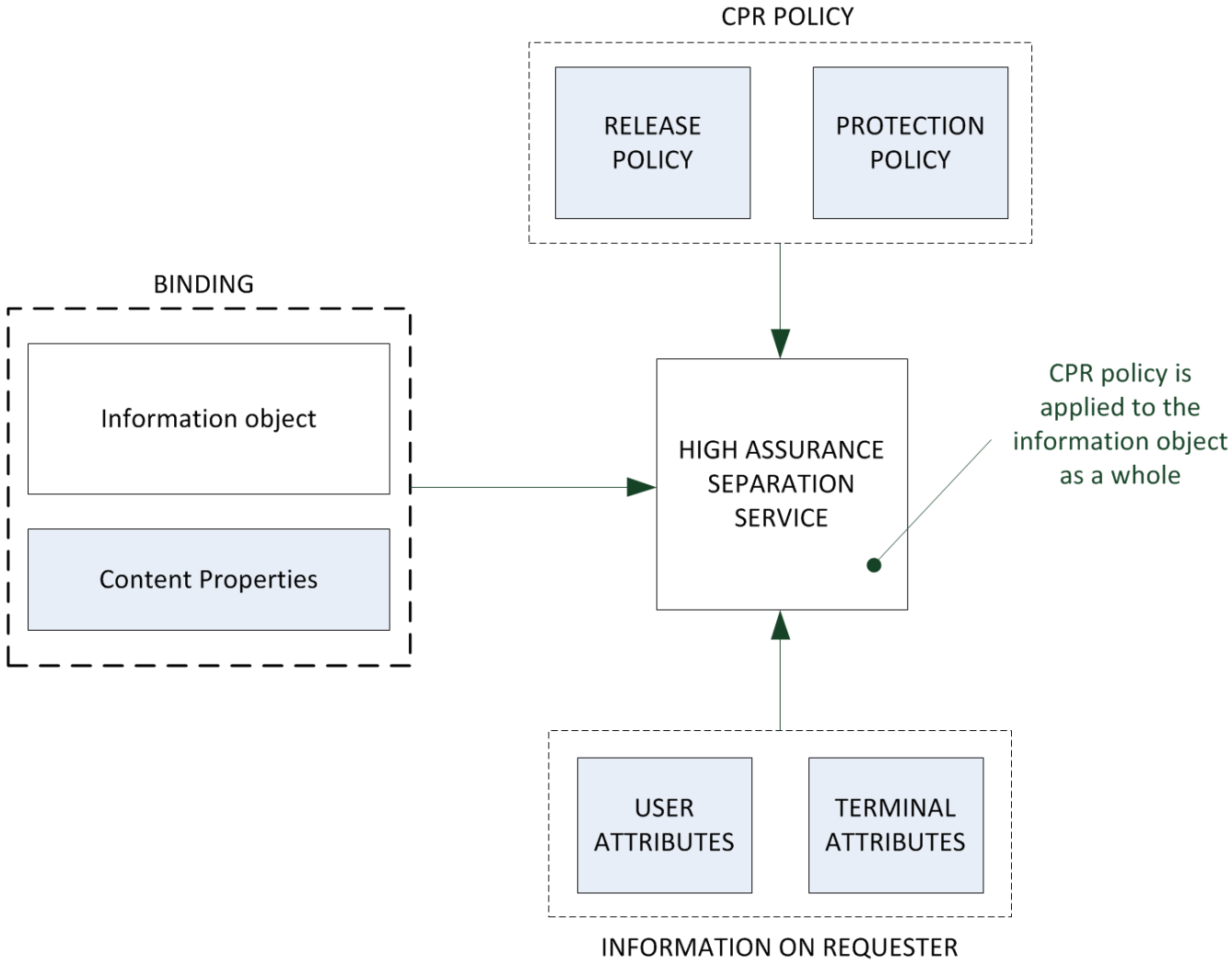
- Enforced during the query
- Requires an enforcement service / gateway
- All access related attributes have to be available at the request time



Network-centric security



From network-centric security to data-centric security: CPR protection model

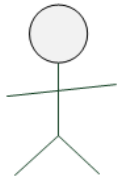


Two approaches to access control: Cryptographic access control

- Symmetric or assymmetric encryption
- The release decision => release of the encryption key
- Can happen before or after data has been produced

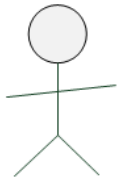
Attribute-based Encryption

1. Setup:
ABE authority generates public parameters *PK* and the secret master key *MK*. The ABE Authority publishes *PK*.


USER A

2. Encryption:
User A encrypts a message M with the public parameters *PK* and based on a set of attributes *S* . The output is the ciphertext M'.

3. Private key request
User B requests a private key *SK* from the ABE Authority for the set *S'* of attributes that user B possesses.


USER B

4. Private key generation
The ABE authority generates the private key *SK* with the secret master key *MK* and based on the set of attributes S', and returns *SK* to User B.

5. Decryption
User B decrypts *M'* with *SK*. If *S'* matches *S* then the output will be the message *M*.

Cryptographic access control