XML Security

Outline

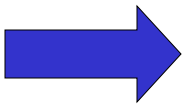
- Security requirements for web data.
- Basic concepts of XML
- Security policies for XML data protection and release
- Access control mechanisms for XML data
- XML-based specification of security informaiton
- XML security: future trends

Web Data: Protection Requirements

- The web is becoming the main information dissemination means for many organizations
- Strong need for models and mechanisms enabling the specification and enforcement of security policies for web data protection and release

Web Docs: Protection Requirements

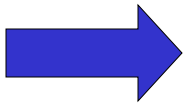
- Web documents may have a nested or hierarchical, inter-linked structure
- Different portions of the same document may have different protection requirements



We need a wide spectrum of *protection granularity levels*

Web Docs: Protection Requirements

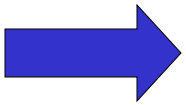
- Web documents may have an associated description of their structure:
  - DTDs and XML Schemas for XML documents
  - Data models for describing the logical organization of data into web pages



Policies specified both at the schema and at the instance level

Web Docs: Protection Requirements

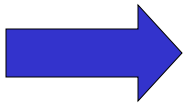
- Documents with the same type and structure may have contents of different sensitivity degree:



Policies that take the document content into account (content-based policies)

Web Docs: Protection Requirements

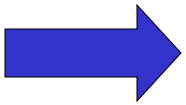
- Supporting fine-grained policies could lead to the specification of a, possibly high, number of access control policies:



Need of mechanisms for *exception management* and *authorization propagation*

Web Docs: Protection Requirements

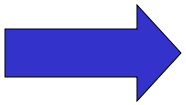
- Heterogeneity of subjects:
  - Subjects accessing a web source may be characterized by different skills and needs and may dynamically change
  - Conventional identity-based access control schemes are not enough



Credentials based on subject characteristics and qualifications

Web Docs: Protection Requirements

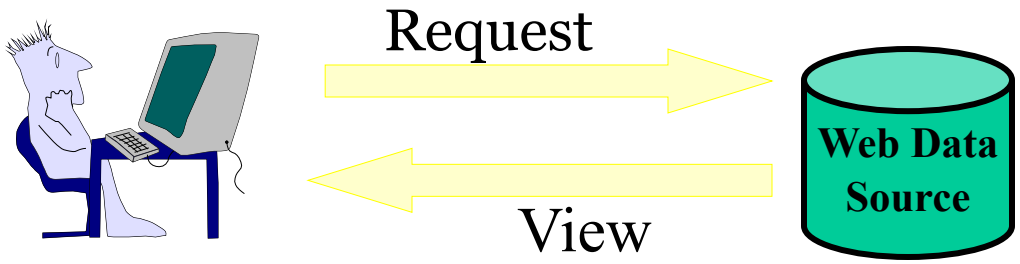
- In a web environment the traditional on user-demand mode of performing access control is not enough:



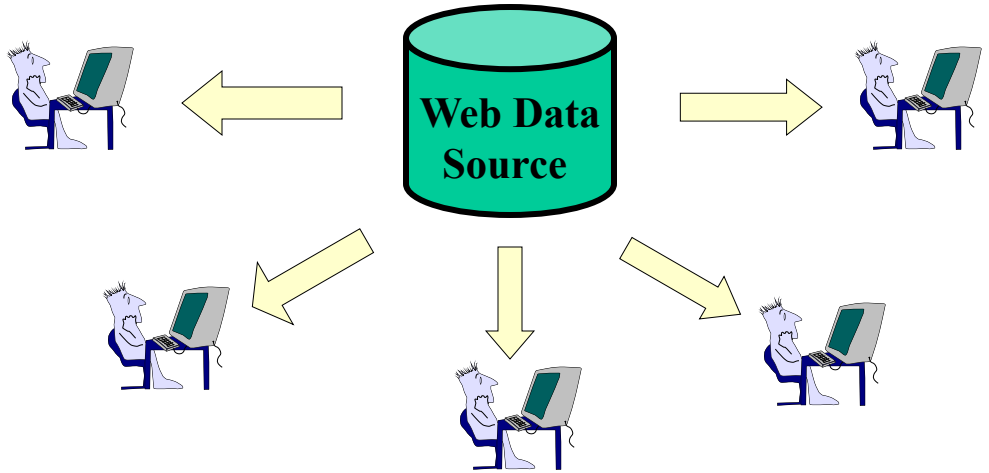
Security policies enforcing both the *pull* and *push* dissemination modes

Dissemination Policies

- **PULL**



- **PUSH**



Outline

- Security requirements for web data
- Basic concepts of XML
- Security policies for XML data protection and release
- Access control mechanisms for XML data
- XML-based specification of security information
- XML security: future trends

Why XML?

- Because XML is becoming a standard for data representation over the web
- XML compatibility is thus an important requirement for security policies, models and mechanisms for Web data sources

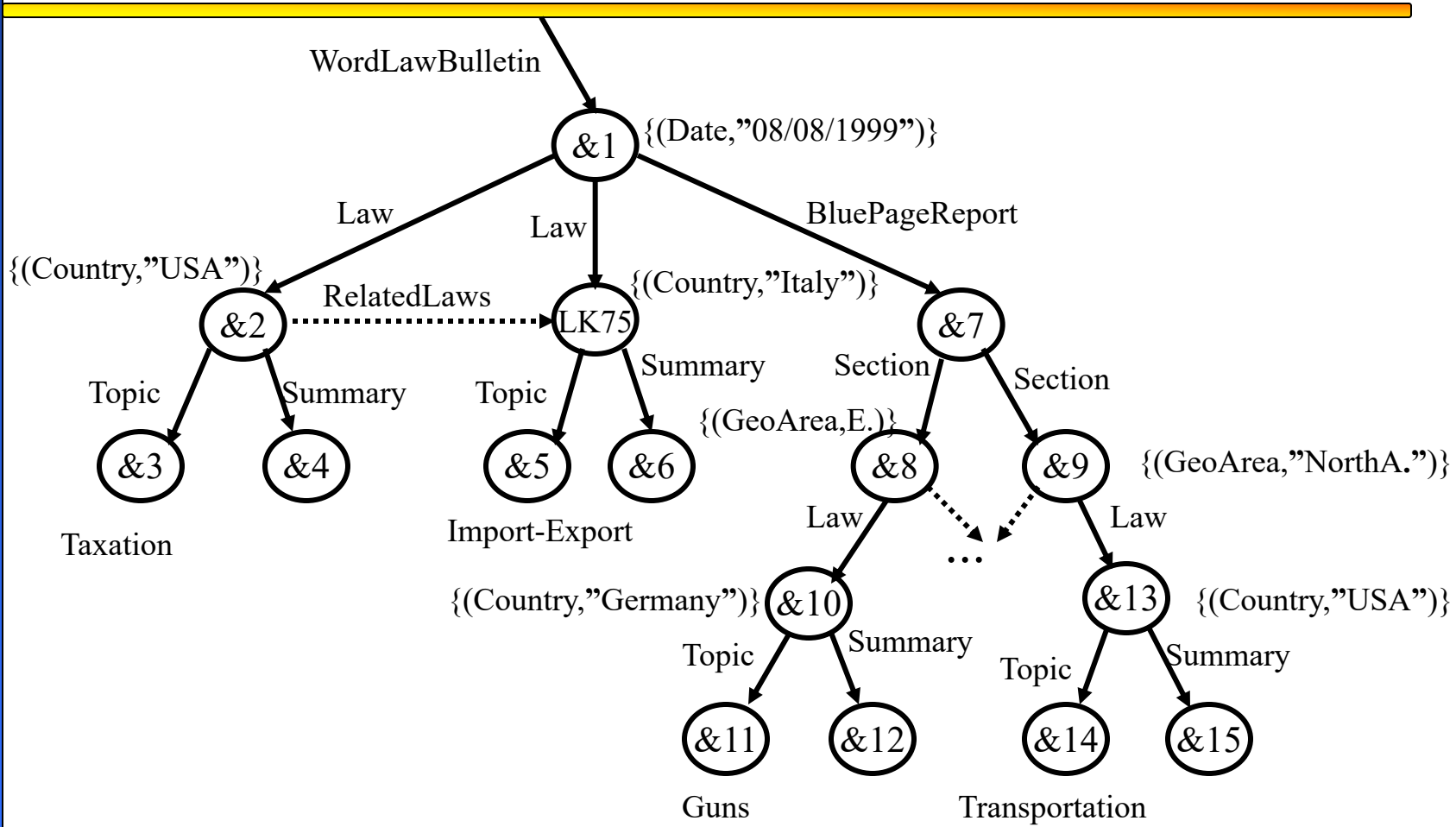
XML

- Building blocks of XML are tagged *elements* that can be nested at any depth in the document structure
- Each tagged element has zero or more *subelements* and zero or more *attributes*
- Elements can be linked by means of *IDREF(S)* attributes
- Optional presence of *a DTD/XMLSchema* for describing the structure of documents (*well-formed* vs *valid* documents)

An XML Document

```
<WorldLawBulletin Date="8/8/1999">
  <Law Country="USA" RelatedLaws = "LK75"/>
      <Topic>Taxation</Topic> <Summary>...</Summary>
  </Law>
  <Law Id="LK75" Country="Italy"/>
      <Topic>Import-Export</Topic> <Summary>...</Summary>
  </Law>
  <BluePageReport>
     <Section GeoArea="Europe">
       <Law Country="Germany"/>
         <Topic>Guns</Topic> <Summary>...</Summary>
       </Law>
       ...
     </Section>
     <Section GeoArea="NorthAmerica">
       <Law Country="USA"/>
         <Topic>Transportation</Topic> <Summary>...</Summary>
       </Law>
       ...
     </Section>
  </BluePageReport>
</WorldLawBulletin>
```

Graph Representation



An XML DTD

```
<!DOCTYPE WorldLawBulletin[
<!ELEMENT WorldLawBulletin (Law*,BluePageReport?)>
<!ELEMENT Law (Topic,Summary)>
<!ELEMENT Topic (#PCDATA)>
<!ELEMENT Summary ANY>
<!ELEMENT BluePageReport (Section+)>
<!ELEMENT Section (Law+)>

<!ATTLIST WorldLawBulletin Date CDATA #REQUIRED>
<!ATTLIST Law Id ID #REQUIRED
              Country CDATA #REQUIRED
              RelatedLaws IDREFS #IMPLIED>
<!ATTLIST Section GeoArea CDATA #REQUIRED>
]>
```

XML & Security

Two main issues:

1. Development of access control models, techniques, mechanisms, and systems for protecting XML documents
2. Use of XML to specify security relevant information, (organizational policies, subject credentials, authentication information, encrypted contents)

The Author-*X* Project

Author-*X*

- Java-based system for XML data sources protection
- Security policy design and administration
- Credential-based access control to XML document sources
- Secure document dissemination and update

Author-*X* ACPs

- Set-oriented and document-oriented policies
- Positive and negative policies at different granularity levels, to enforce differentiated protection of XML documents and DTDs
- Controlled propagation of access rights
- ACPs reflect user profiles through credential-based qualifications

Enforcing access control

- Subject specification
- Protection object specification
- Privilege
- Propagation option

Subject Specification

- *User Identifiers*

OR

- *Subject credential*: credential expression

Ex: X.age > 21

Programmer(X) and X.country="Italy"

Protection Object Specification

- Identify the portions of a document(s) to which the authorization applies.

  We want to allow users to specify authorizations ranging from

  – sets of documents

  – to single elements/attributes within documents

specification on DTD or documents

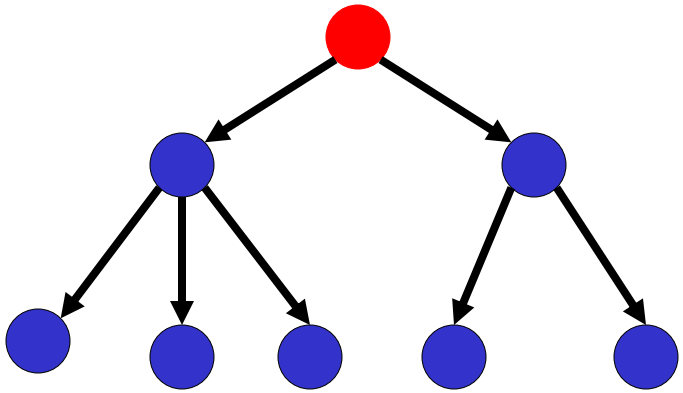
[{doc|*}|{DTD|#}].[pathOfElem|ElemIds].[Attrs|links]

Privileges

- browsing
  - read
  - navigate
- authoring
  - write
  - append
  - delete

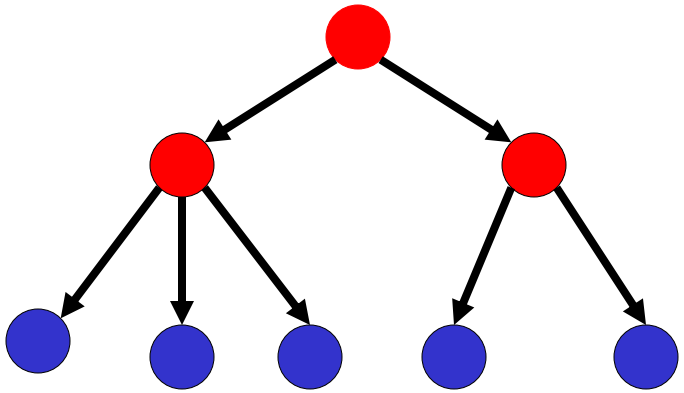
Propagation option

NO PROPAGATION



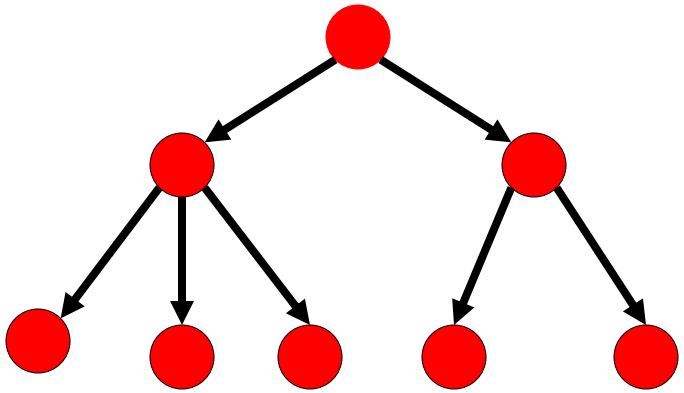
Propagation option

FIRST LEVEL



Propagation option

CASCADE



Examples of authorization rules

P1 = ((LLoC Employee or European Division Employee), WorldLawBulletin.Law, browse_all, *)

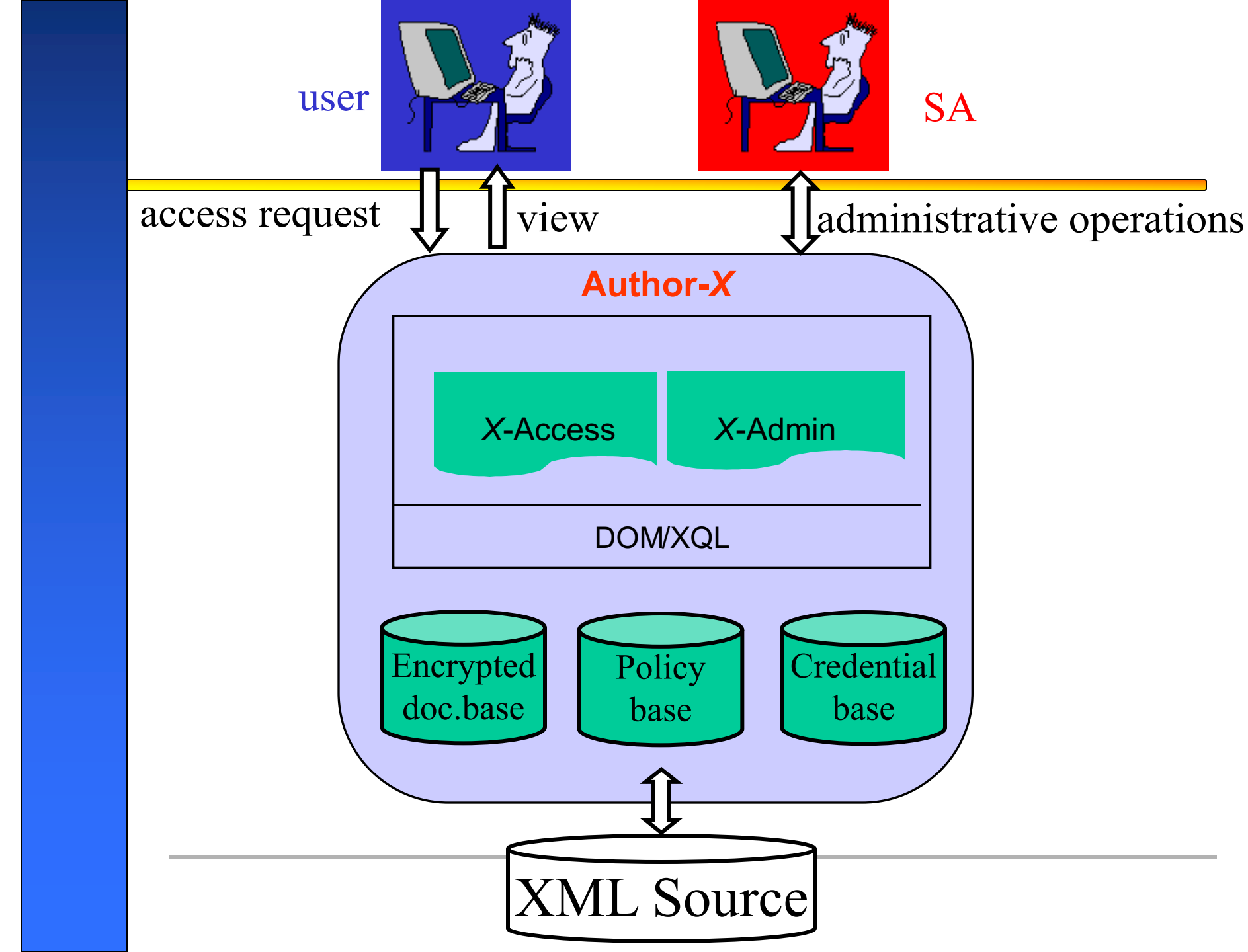
this authorization rule authorizes the LLoC and European Division Employees to view all laws (not contained in the BluePageReport *element) in all instances of* WorldLawBulletin

relations among laws, that is, RelatedLaws *attributes, are also displayed*

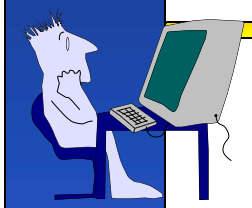
Examples of authorization rules

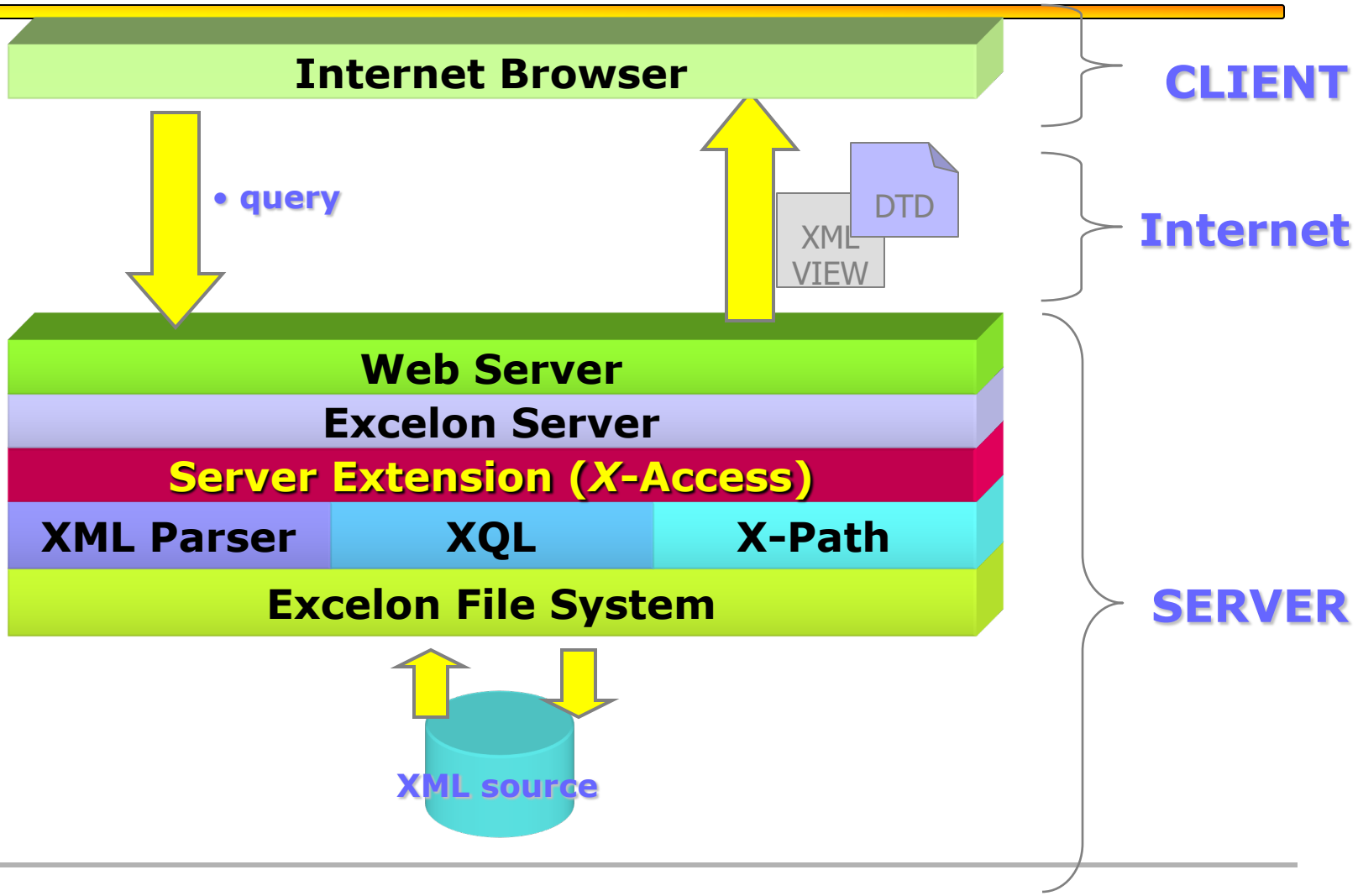
P4 = (European Division Employee,
(WorldLawBulletin.BluePageReport.Section,
GeoArea = Europe), browse_all, *)

this authorization rule authorizes the European Division Employees to view the section pertaining to Europe of the BluePageReport *in all instances of* WorldLawBulletin

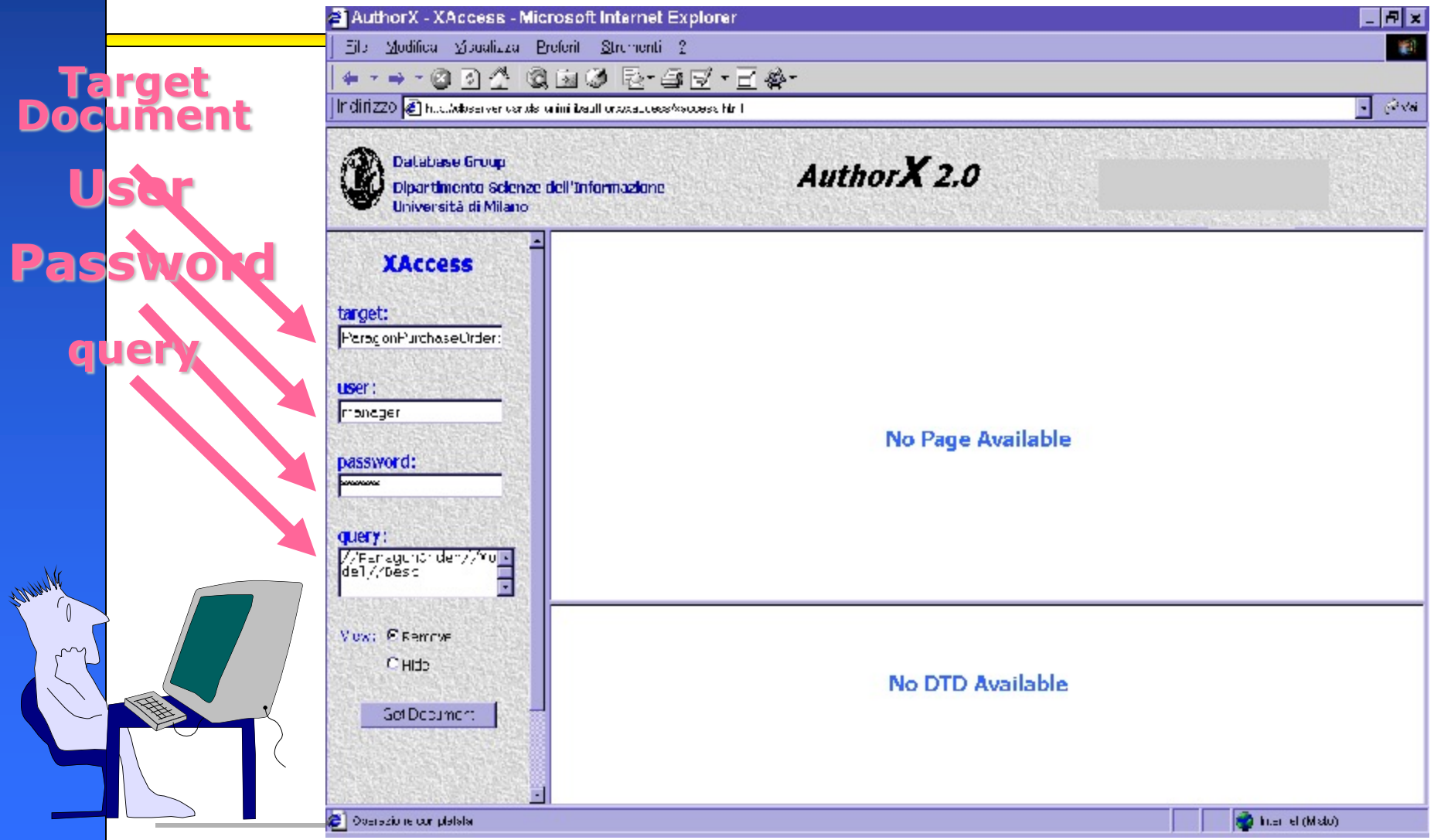

user
SA
access request
view
administrative operations
Author-X
X-Access
X-Admin
DOM/XQL
Encrypted doc.base
Policy base
Credential base
XML Source

Information Pull - Architecture



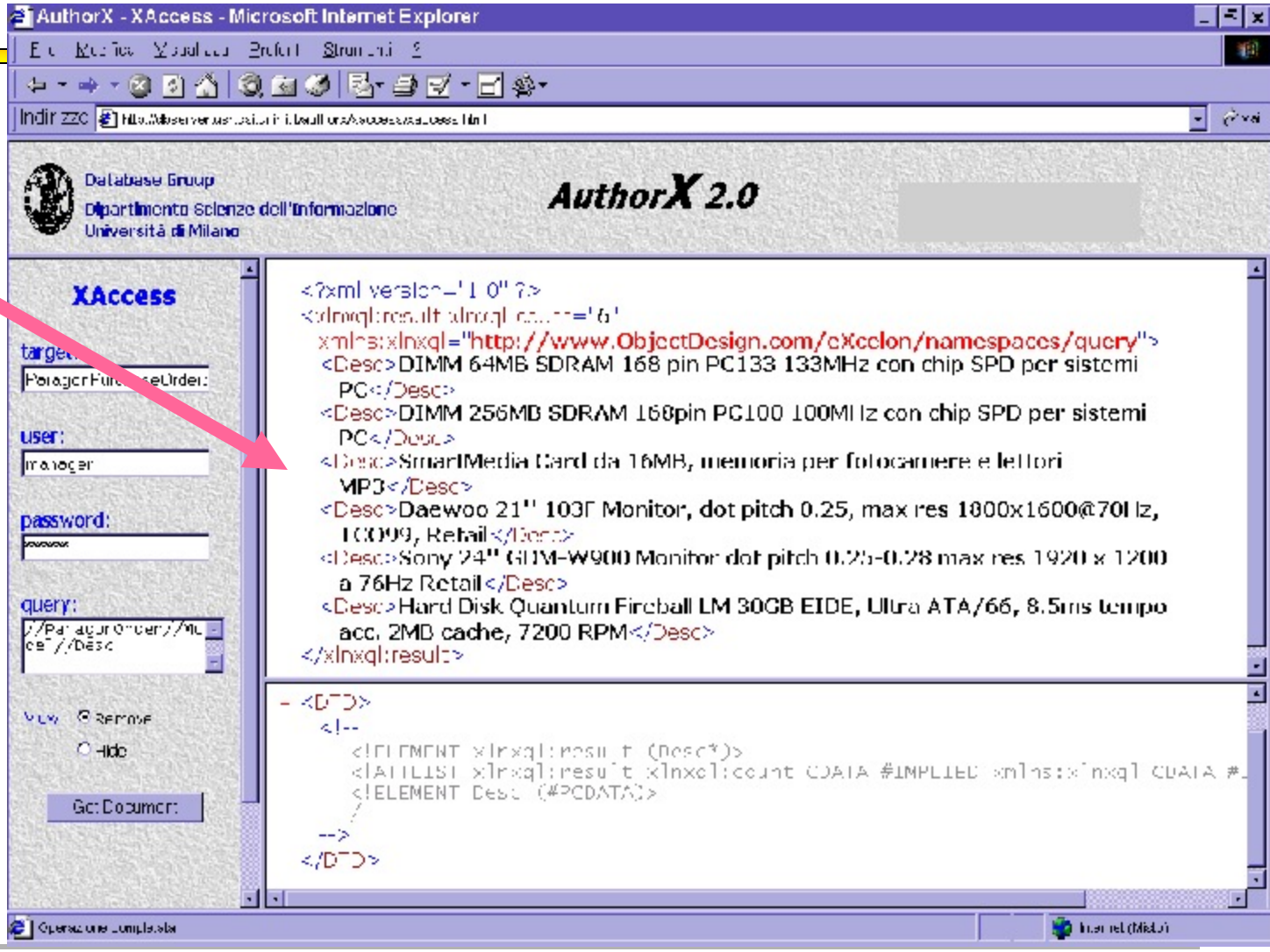


Access request



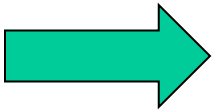
Query result

Query result



Push Dissemination Mode

- Since:
  - Different subjects -> different views
  - Wide range of protection granularities
  - High number of subjects



Number of views can be too large

Solution-> Encryption Techniques

Push Dissemination Mode

- The approach is based on encrypting different portions of the same document with different keys
- The same (encrypted) copy is then broadcasted to all subjects
- Each subject only receives the key(s) for the portions he/she is enabled to see

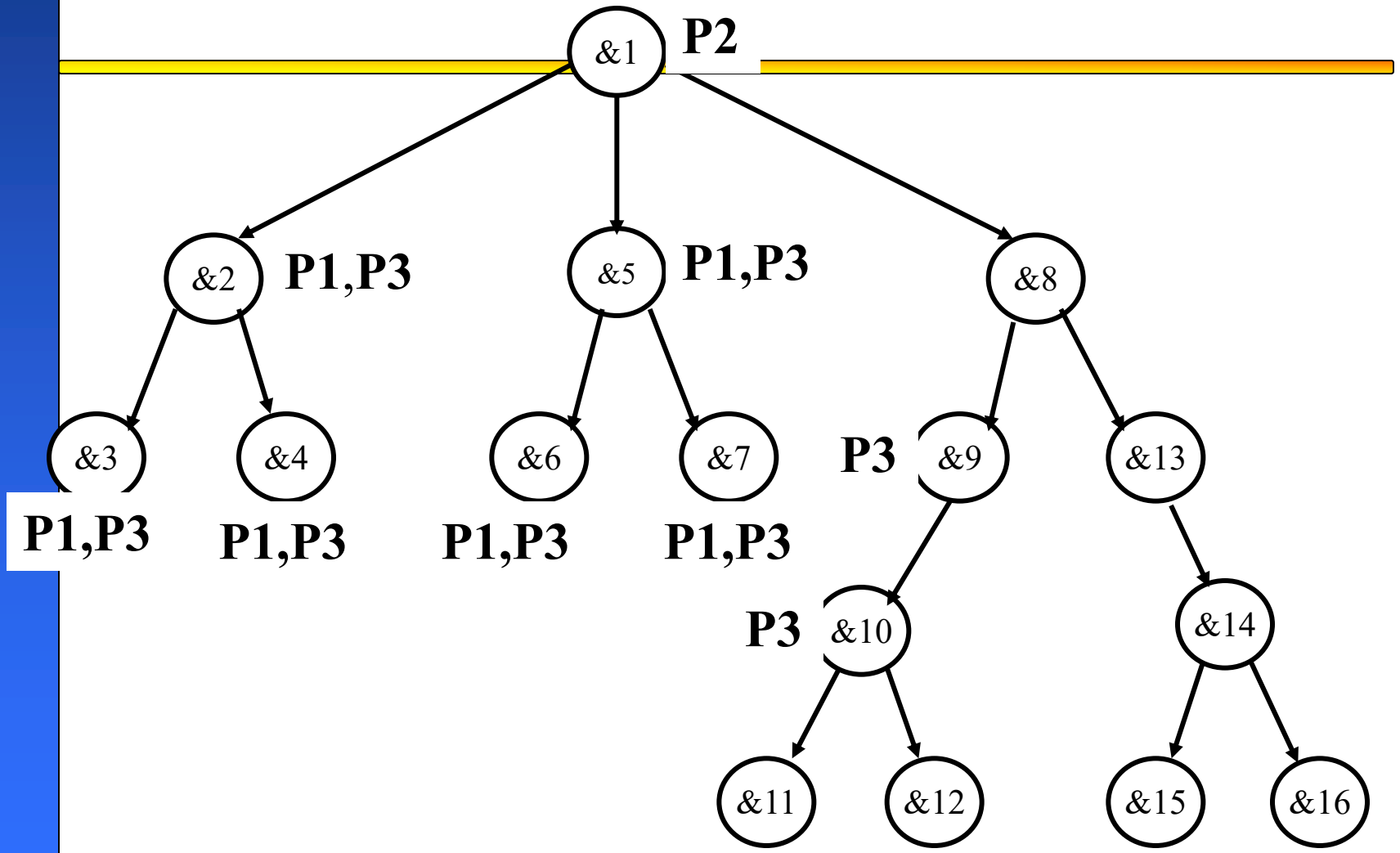
Information Push - Main Issues

- How to encrypt the documents in a source
- Which and how many keys should be distributed to which subjects
- How to securely and efficiently distribute keys to subjects in such a way that keys are received only by the entitled subjects

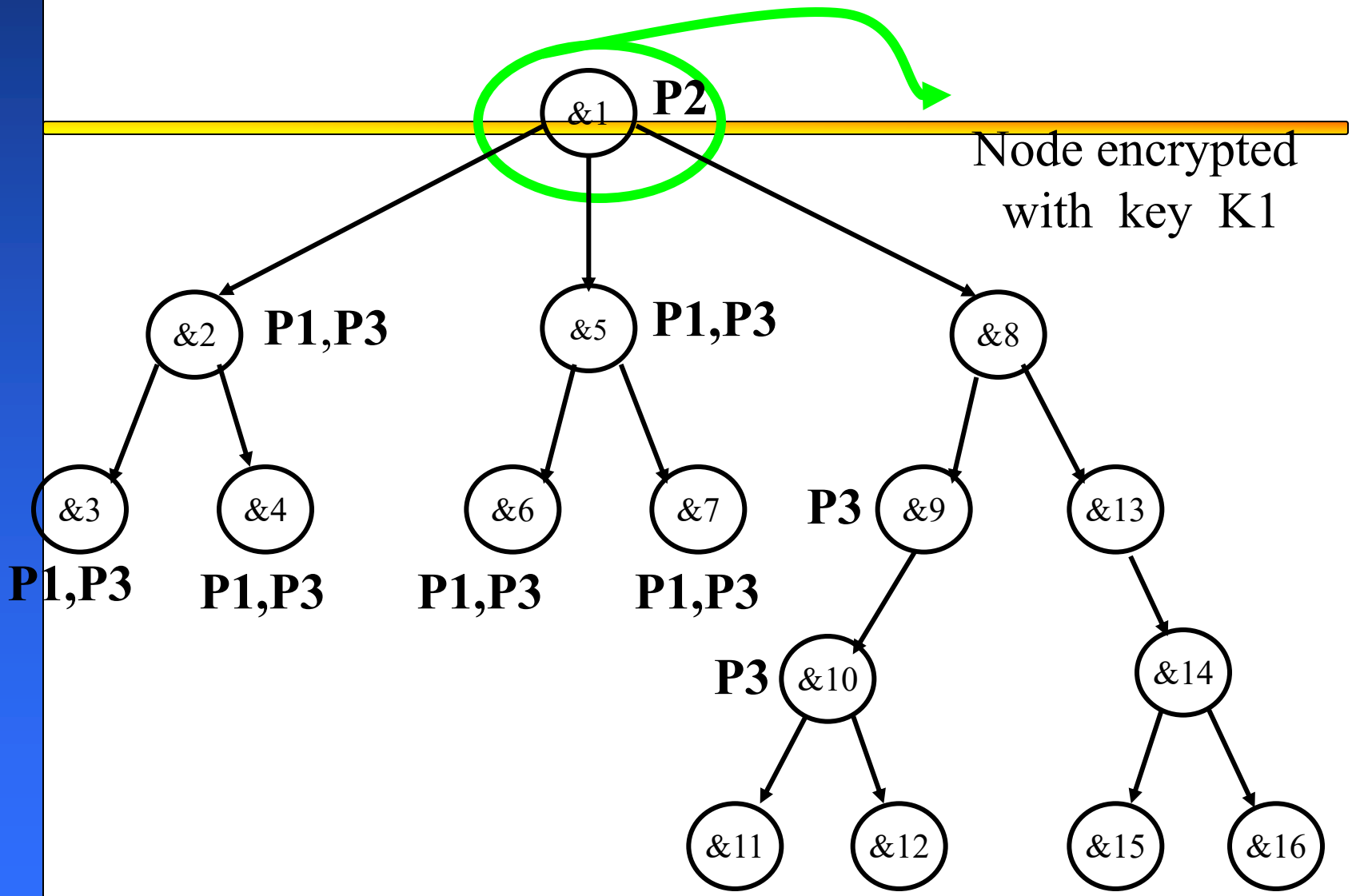
How to Encrypt Documents

- Document encryption is driven by the specified access control policies: all the document portions to which the same access control policies apply are encrypted with the same key
- Thus, to determine which keys should be sent to a particular subject it is only necessary to verify which are the access control policies that apply to that subject and then sending the keys associated with these policies

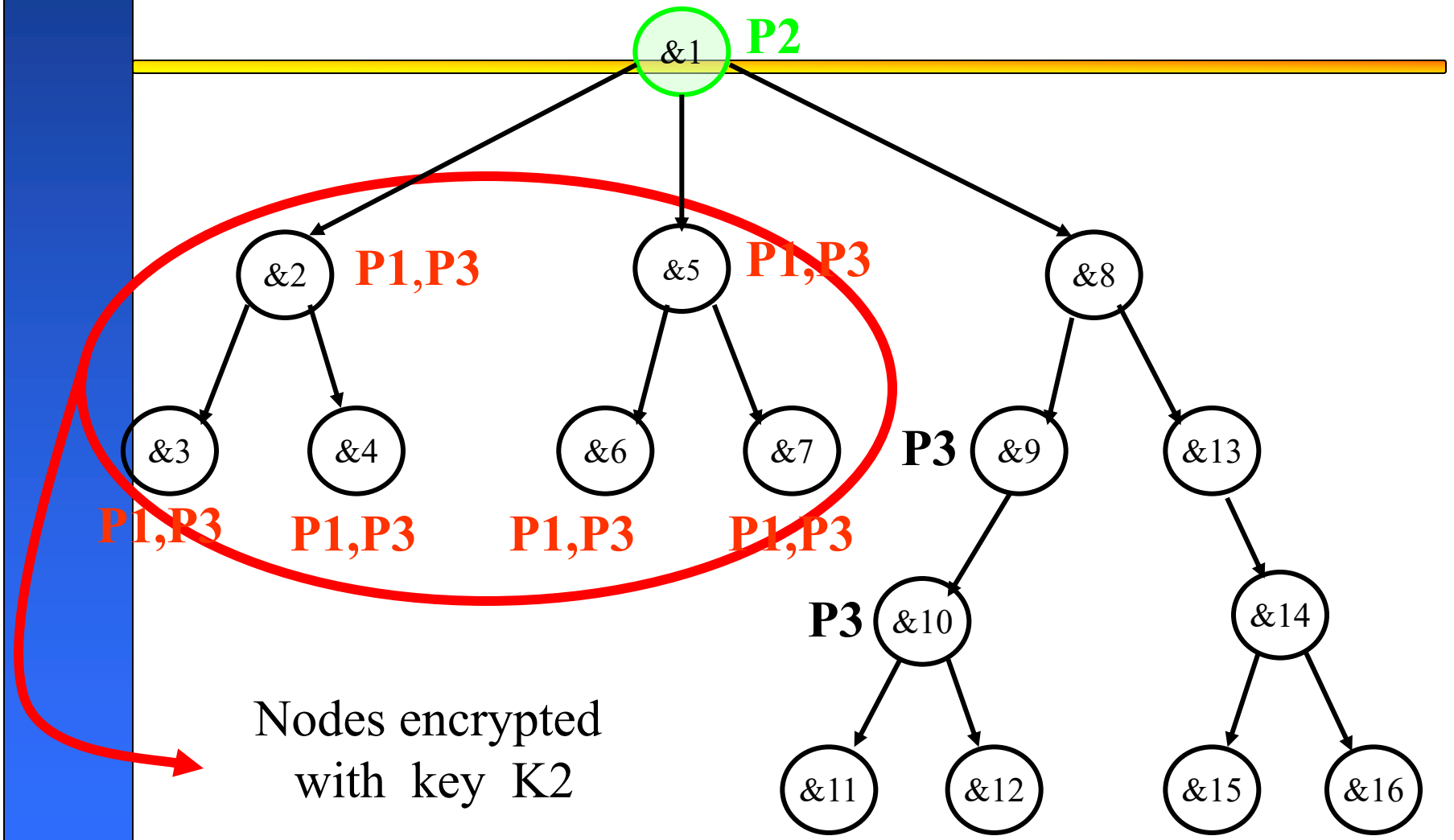
Well-Formed Encryption



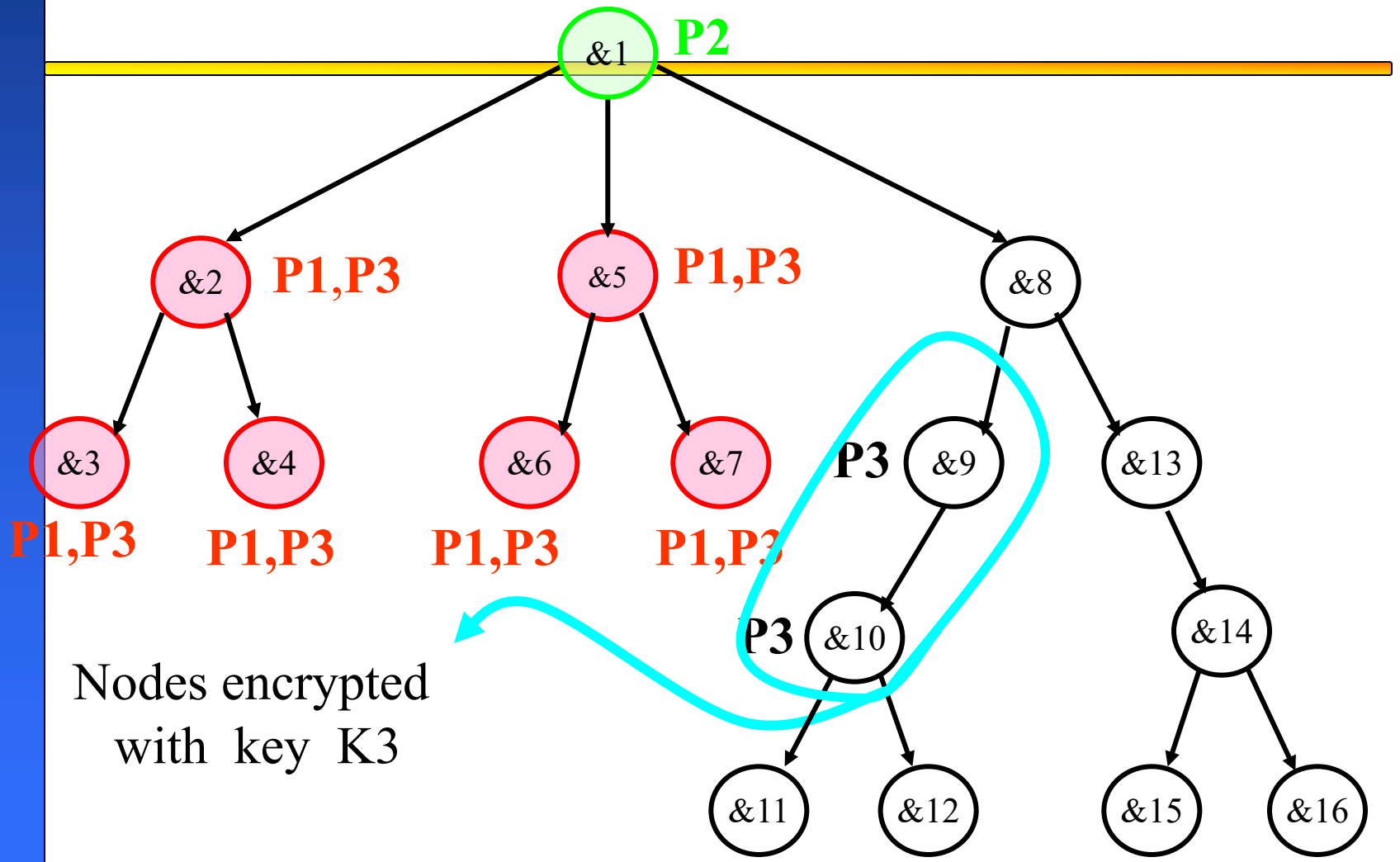
Well-Formed Encryption



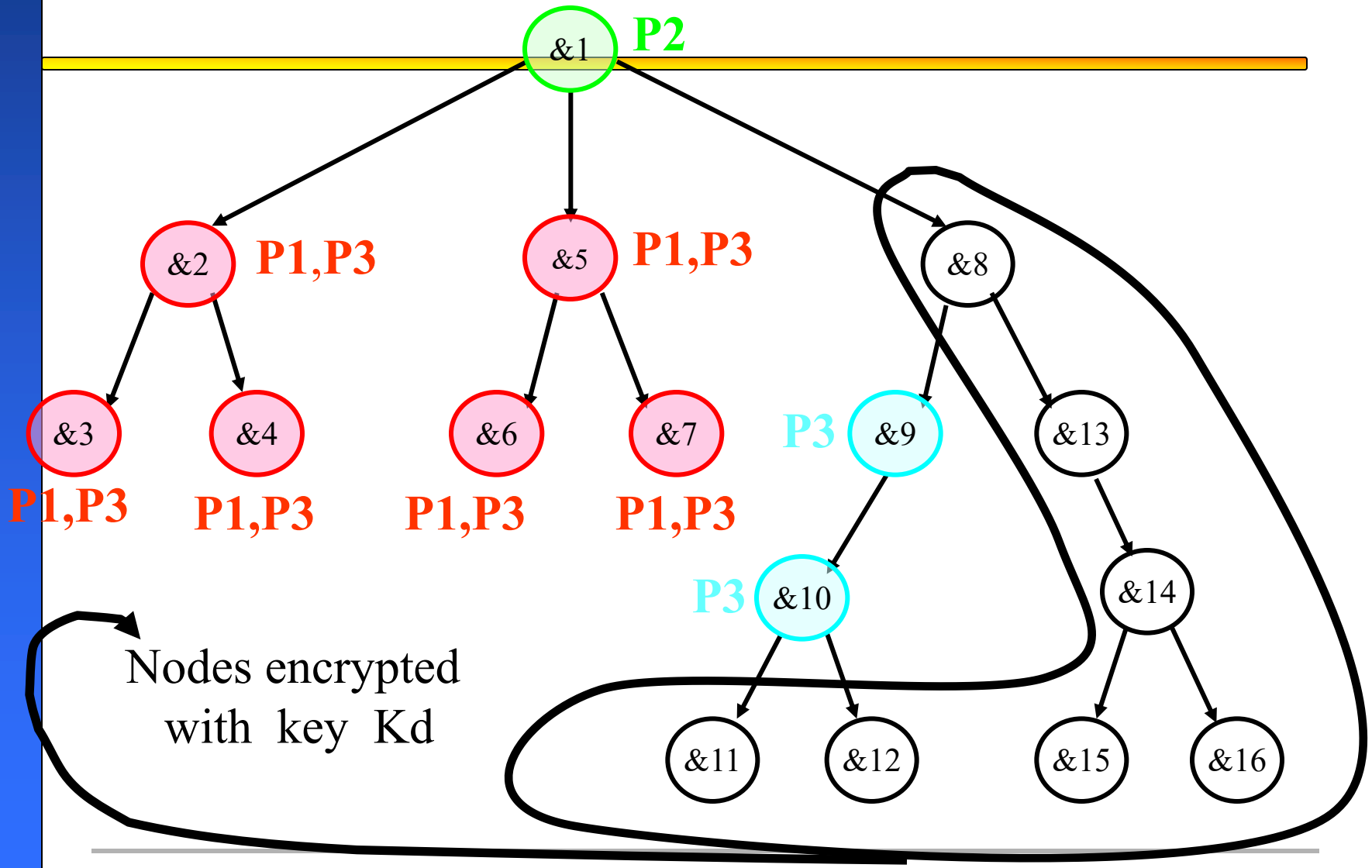
Well-Formed Encryption



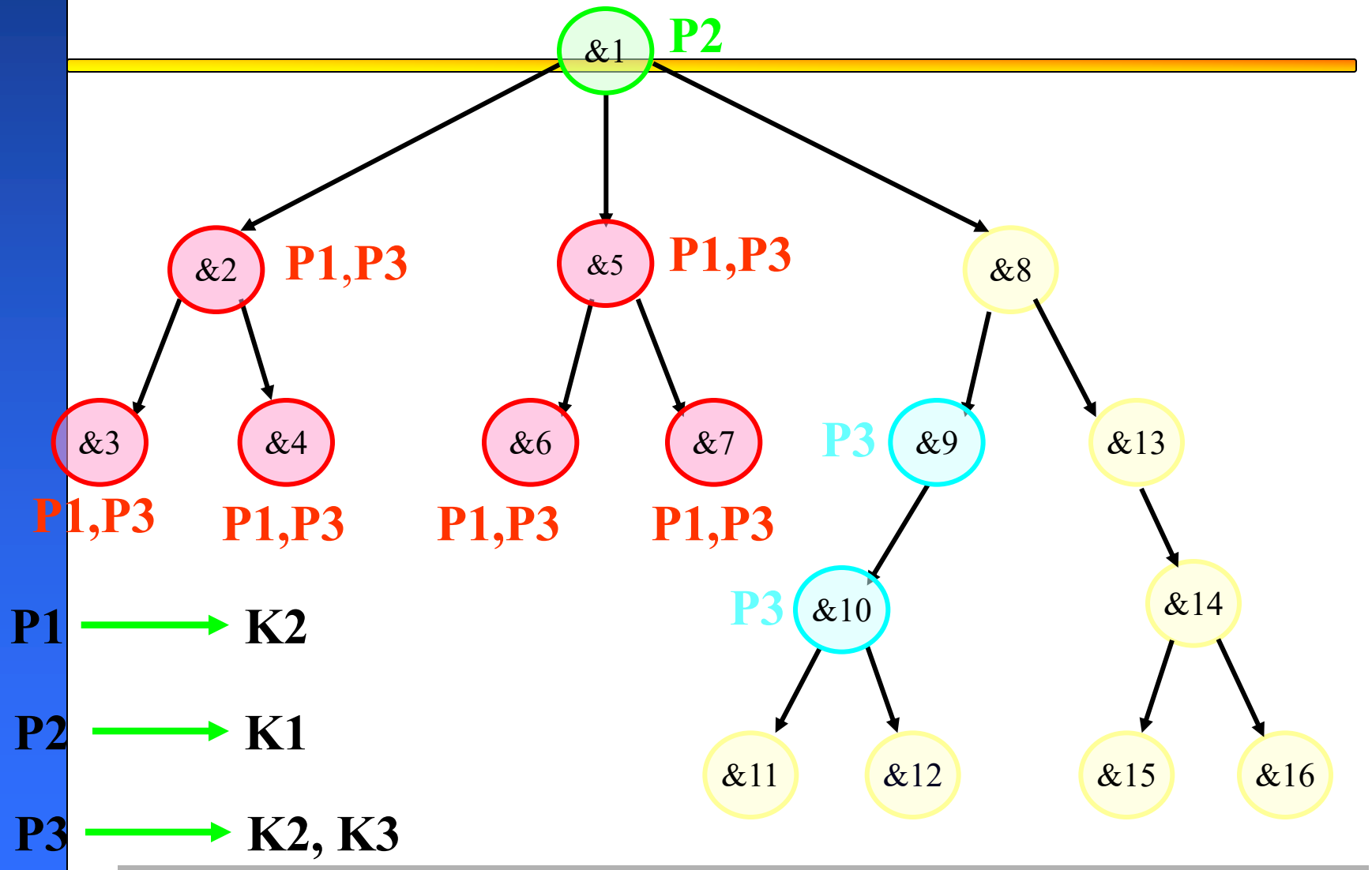
Well-Formed Encryption



Well-Formed Encryption



Well-Formed Encryption



Key Management

- Key assignment scheme such that:
  - From the key associated with a policy P1 it is possible to derive the keys associated with all the policy configurations containing P1
- Benefits:
  - The system should manage in the worst case a number of keys equal to the size of the Policy Base
  - Each subject receives a key for each policy he/she satisfies

Outline

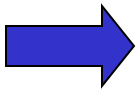
- Security requirements for web data
- Basic concepts of XML
- Security policies for XML data protection and release
- Access control mechanisms for XML data
- XML-based specification of security information
- XML security: future trends

Why?

- It allows a uniform protection of XML documents and their security-related information
- It facilitates the export and exchange of security information

Goals

- Definition of an XML-based language for specifying security-related information for web documents:
  - Subject credentials
  - Access control policies for web documents satisfying the previously stated requirements



An example: *X*-Sec the XML-based language developed in the framework of Author-*X*

X-Sec Credentials

- Credentials with similar structure are grouped into credential types
- A credential is a set of simple and composite properties
- Credential types → DTDs
- Credentials → XML documents

X-Sec credential type

```
<!DOCTYPE carrier_employee[
<!ELEMENT carrier_employee (name,address,phone_number*,
                            email?, company)>
<!ELEMENT name (fname,lname)>
<!ELEMENT address (#PCDATA)>
<!ELEMENT phone_number (#PCDATA)>
<!ELEMENT email (#PCDATA)>
<!ELEMENT company (#PCDATA)>
<!ATTLIST carrier_employee credID ID #REQUIRED
                           cIssuer CDATA #REQUIRED>
]>
```

X-Sec credential

```
<carrier_employee credID="154",CIssuer="CA16">
  <name>
      <fname> Bob  </fname>
       <lname> Watson </lname>
   </name>
  <address> 24 Baker Street </address>
   <phone_number> 8005769840 </phone_number>
   <email> bwatson@ups.com </email>
   <company> UPS  </company>
</carrier_employee>
```

X-Sec Policy Specification

- XML template for specifying credential-based access control policies
- The template is as general as possible to be able to model access control policies for a variety of web documents (e.g., HTML, XML)

X-Sec Policy Base Template

```
<!DOCTYPE policyBase[
<!ELEMENT policyBase (policySpec)*>
<!ELEMENT policySpec  (subject, object, priv, type, prop)>
<!ELEMENT subject (userID*|credential)>
<!ELEMENT object EMPTY>
<!ELEMENT priv EMPTY>
<!ELEMENT type EMPTY>
<!ELEMENT prop EMPTY>
<!ELEMENT userID EMPTY>
<!ELEMENT credential EMPTY>
<!ATTLIST userID id CDATA #REQUIRED>
<!ATTLIST credential targetCredType CDATA #REQUIRED credExpr CDA
IMPLIED>
<!ATTLIST object target CDATA #REQUIRED path CDATA #REQUIRED>
<!ATTLIST userID id CDATA #REQUIRED>
<!ATTLIST priv value CDATA #REQUIRED>
<!ATTLIST type value CDATA #REQUIRED>
<!ATTLIST prop value CDATA #REQUIRED>
]>
```

Instantiation for XML Sources

```
<policyBase>
  <policySpec>
    <subject><credential targetCredType="ACMmember"/></subject>
    <object>< target="SigmodRecord.xml" path="/issues"/></object>
    <priv value="READ"/> <type value="grant"/> <prop
value="cascade"/>
  </policySpec>

  <policySpec>
    <subject><credential targetCredType="noACMmember"/></subject>
    <object>< target="SigmodRecord.xml" path="/issues"/></object>
    <priv value="READ"/> <type value="grant"/> <prop
value="cascade"/>
  </policySpec>

  <policySpec>
    <subject><credential targetCredType="noACMmember"/></subject>
    <object>< target="SigmodRecord.xml" path
="/issues/issuesTuple/articles/
                    articlesTuple/abstract"/></object>
    <priv value="READ"/> <type value="deny"/> <prop
value="no_prop"/>
 </policySpec>
 </policyBase>
```

Outline

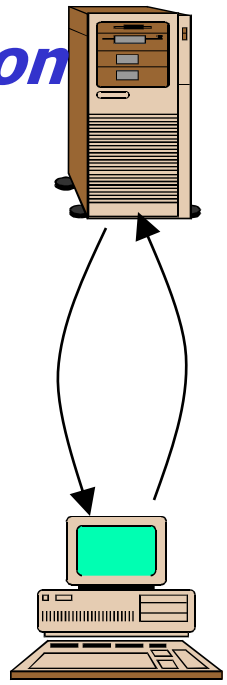
- Security requirements for web data
- Basic concepts of XML
- Security policies for XML data protection and release
- Access control mechanisms for XML data
- XML-based specification of security information
- XML security: future trends

Research Trends

- Secure publishing of XML documents:
  - A new class of information-centered applications based on ***Data dissemination***
  - Possible scenarios:
    - Information commerce: digital libraries, electronic news
    - Intra-company information systems
- Security requirements:
  - Confidentiality
  - Integrity
  - Authenticity
  - Completeness

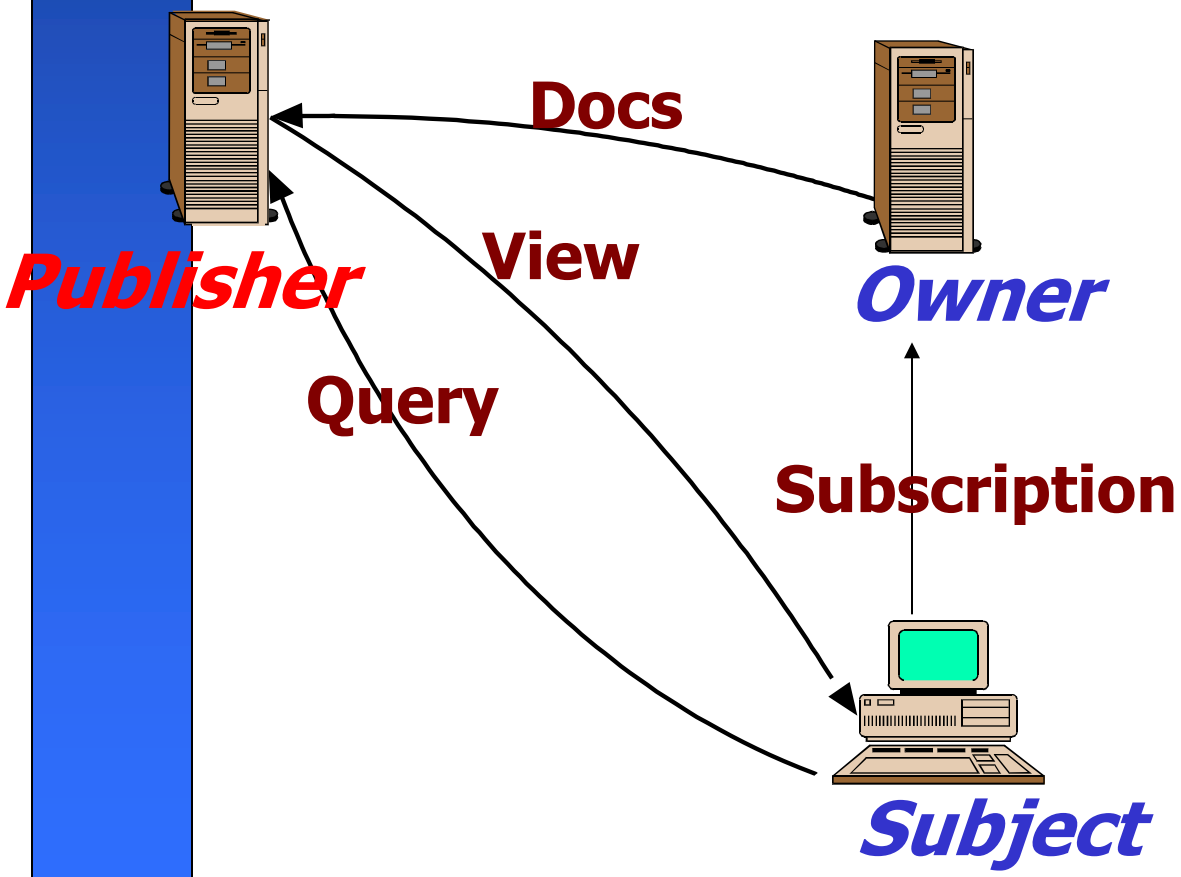
Secure Publishing

Traditional Architecture



- **The Owner is the producer of information**
- **It specifies access control policies**
- **It answers to subject queries**

Third-Party Architecture



- The Publisher is responsible for managing (a portion of) the Owner information and for answering subject queries
- Benefits:
  - Scalability
  - No Bottleneck

Main References

- B. Dournee, XML Security, *RSA Press*, 2002.
- E. Bertino, B. Carminati, E. Ferrari, and B. Thuraisingham, XML Security, *Addison-Wesley*, in preparation.

Main References

- E. Bertino and E. Ferrari. Secure and Selective Dissemination of XML Documents, *ACM Trans. on Information System and Security*, to appear
- E. Bertino, S. Castano, e E. Ferrari. Author- *X*: a Comprehensive System for Securing XML Documents, *IEEE Internet Computing*, May 2001
- E. Bertino, S. Castano, e E. Ferrari. Securing XML Documents: the Author-X Project Demonstration, Proc. of the *ACM SIGMOD Conference 2001*
- E. Bertino, S. Castano, E. Ferrari, M. Mesiti. Specifying and Enforcing Access Control Policies for XML Document Sources. *World Wide Web Journal,* 3(3), 2000

Main References

- Web sites:
  - The XML Security Page: http://www.nue.et-inf.uni-siegen.de/~geuer-pollmann/ xml/security.html
  - OASIS Consortium**:** http://www.oasis-open.org
  - World Wide Web Consortium: http://www.w3.org