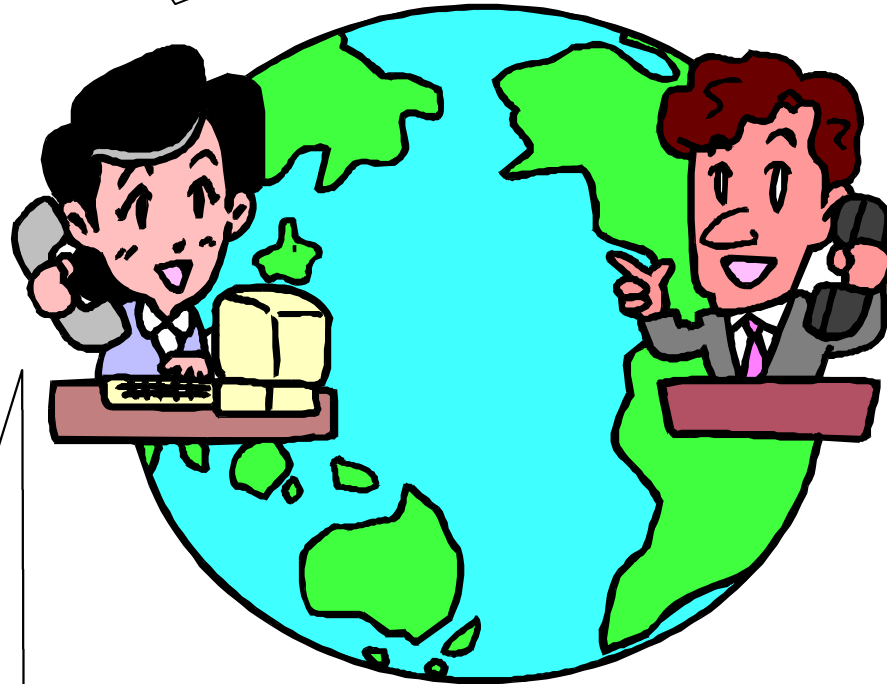


SECURITY ON THE INFORMATION HIGHWAY



Jeanne Proulx and Lucie Goulet, attorneys
Ministère de la justice
Direction des affaires juridiques et législatives
September 3, 1999

WHAT CAN THE LEGISLATOR DO?



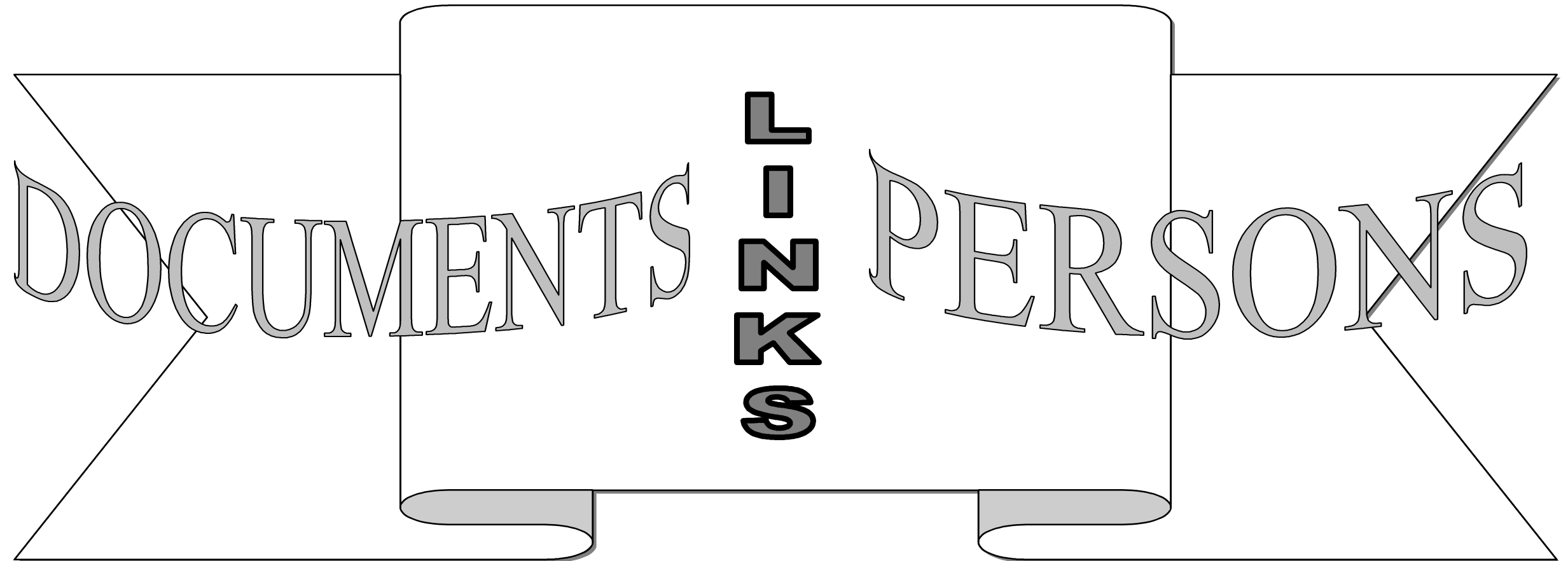
**CONFIDENCE IN
WHOM? IN WHAT?**

**MAKE SURE THAT PEOPLE
HAVE ENOUGH CONFIDENCE
TO DEAL WITH EACH OTHER
AND WITH THE
GOVERNMENT**

**CONFIDENCE IN PEOPLE USING
ELECTRONIC SUPPORTS TO
COMMUNICATE**

**CONFIDENCE IN THE INTEGRITY
OF DOCUMENTS AND IN THEIR
ELECTRONIC SUPPORTS**

AXIS OF THE LEGAL INFRASTRUCTURE

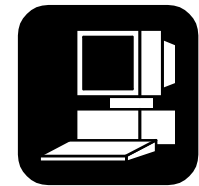
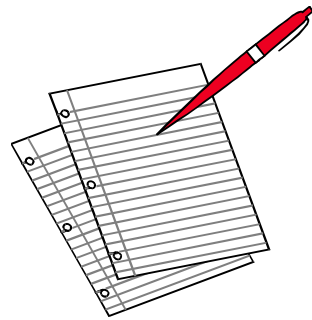


THE DOCUMENT

FEATURES COMMON TO ALL DOCUMENTS:

A document is a:

- ❖ **MATERIAL**
- ❖ **DELIMITED**
- ❖ **STRUCTURED**
- ❖ **OBJECT**



HARD COPY

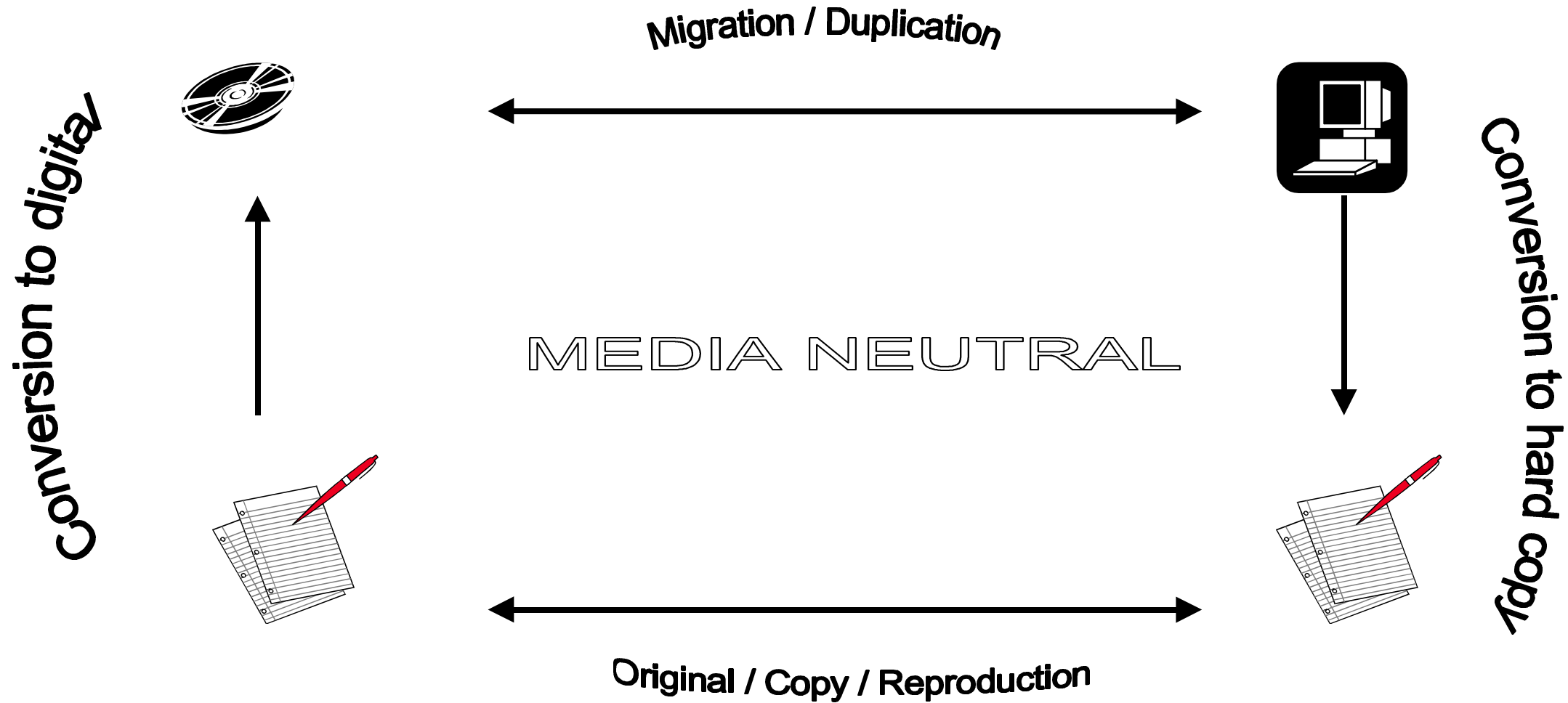
INTERCHANGEABILITY OF SUPPORTS

FUNCTIONAL EQUIVALENCE

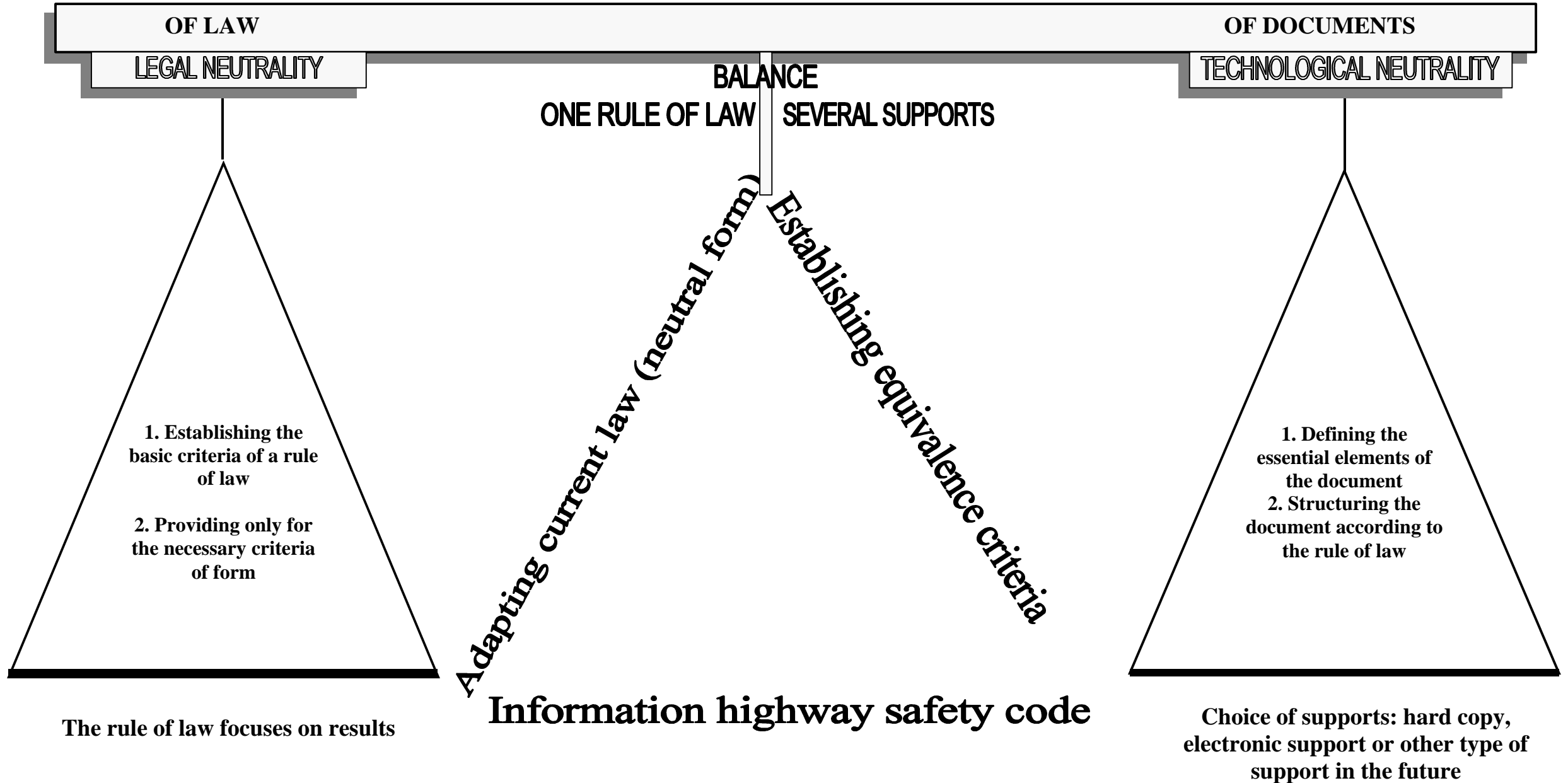
ELECTRONIC COPY

INTEGRITY OF A DOCUMENT DURING ITS LIFE CYCLE

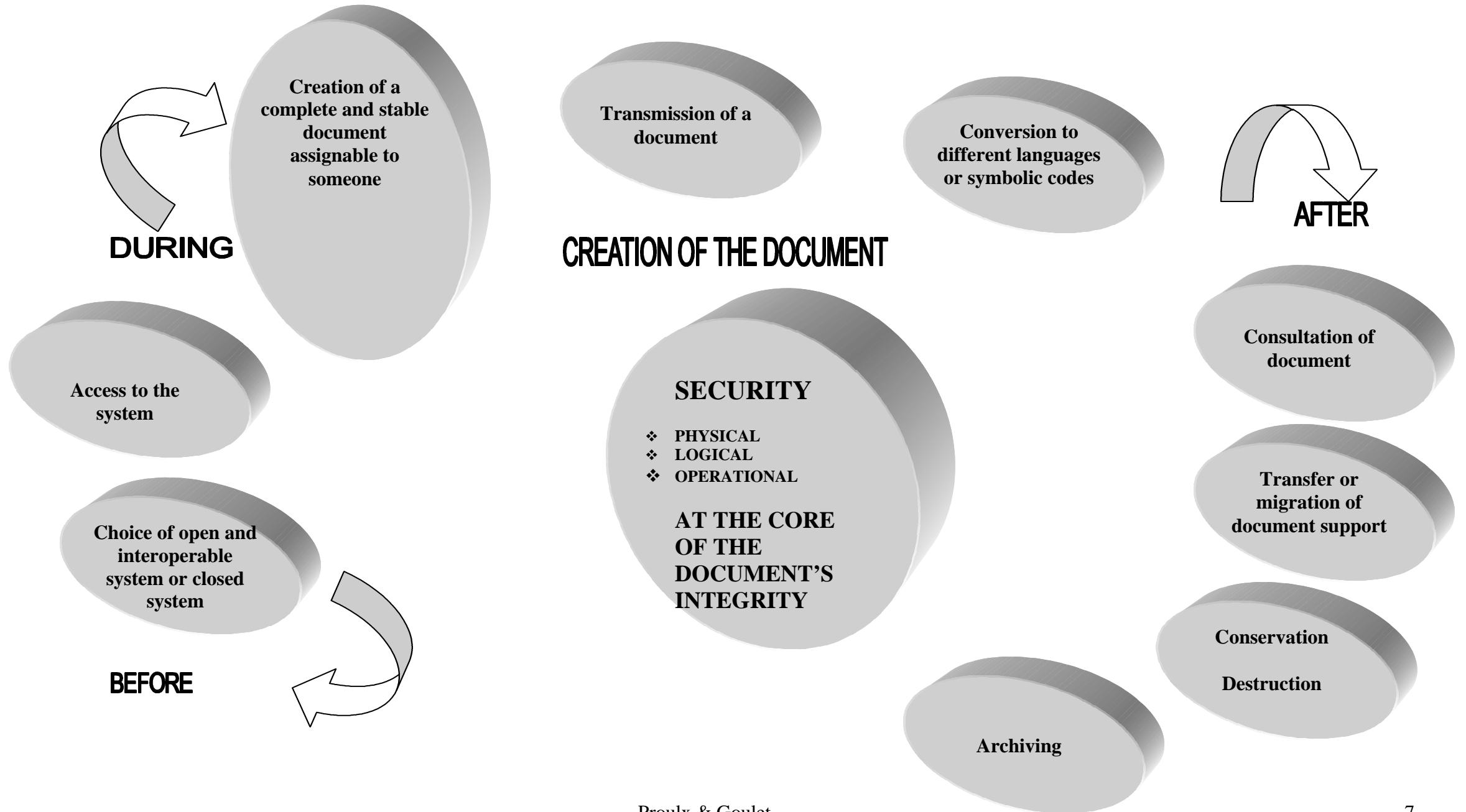
INTERCHANGEABILITY OF SUPPORTS



FUNCTIONAL EQUIVALENCE

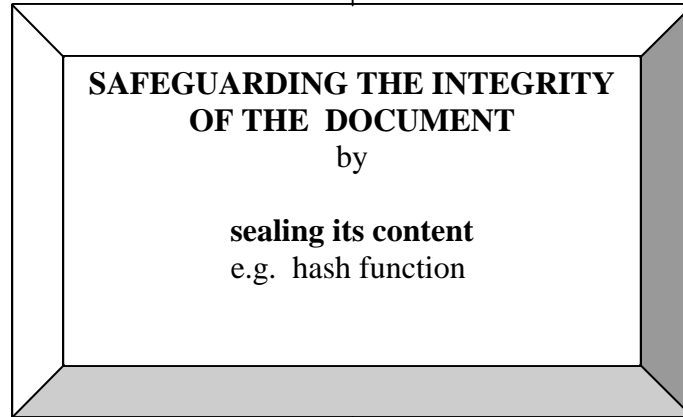


INTEGRITY OF A DOCUMENT DURING ITS LIFE CYCLE

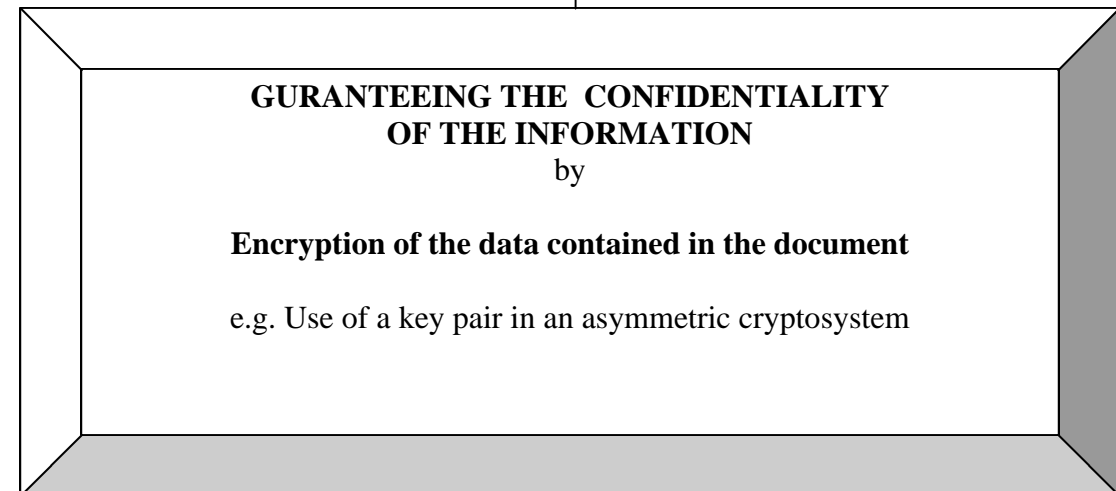
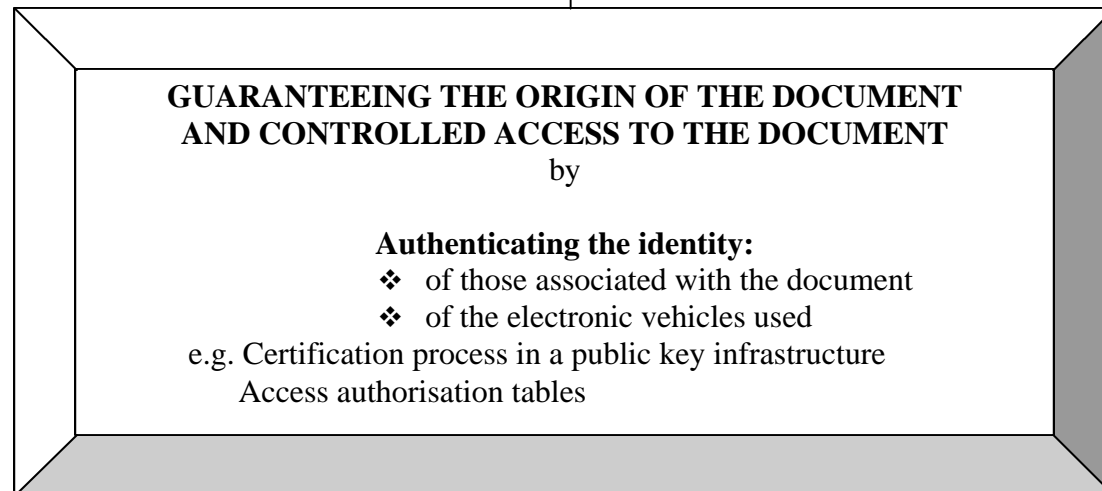
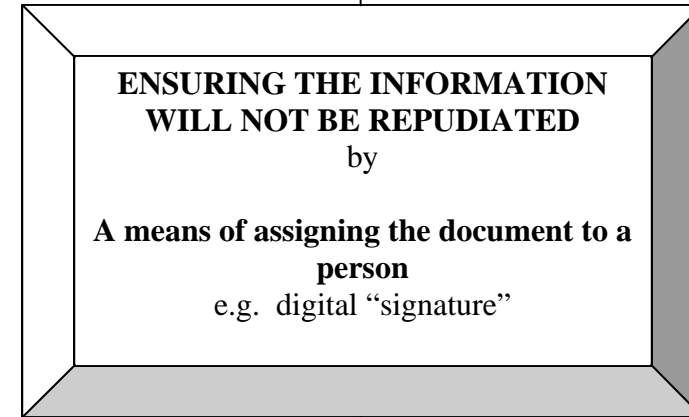


TECHNOLOGY AT THE SERVICE OF SECURITY

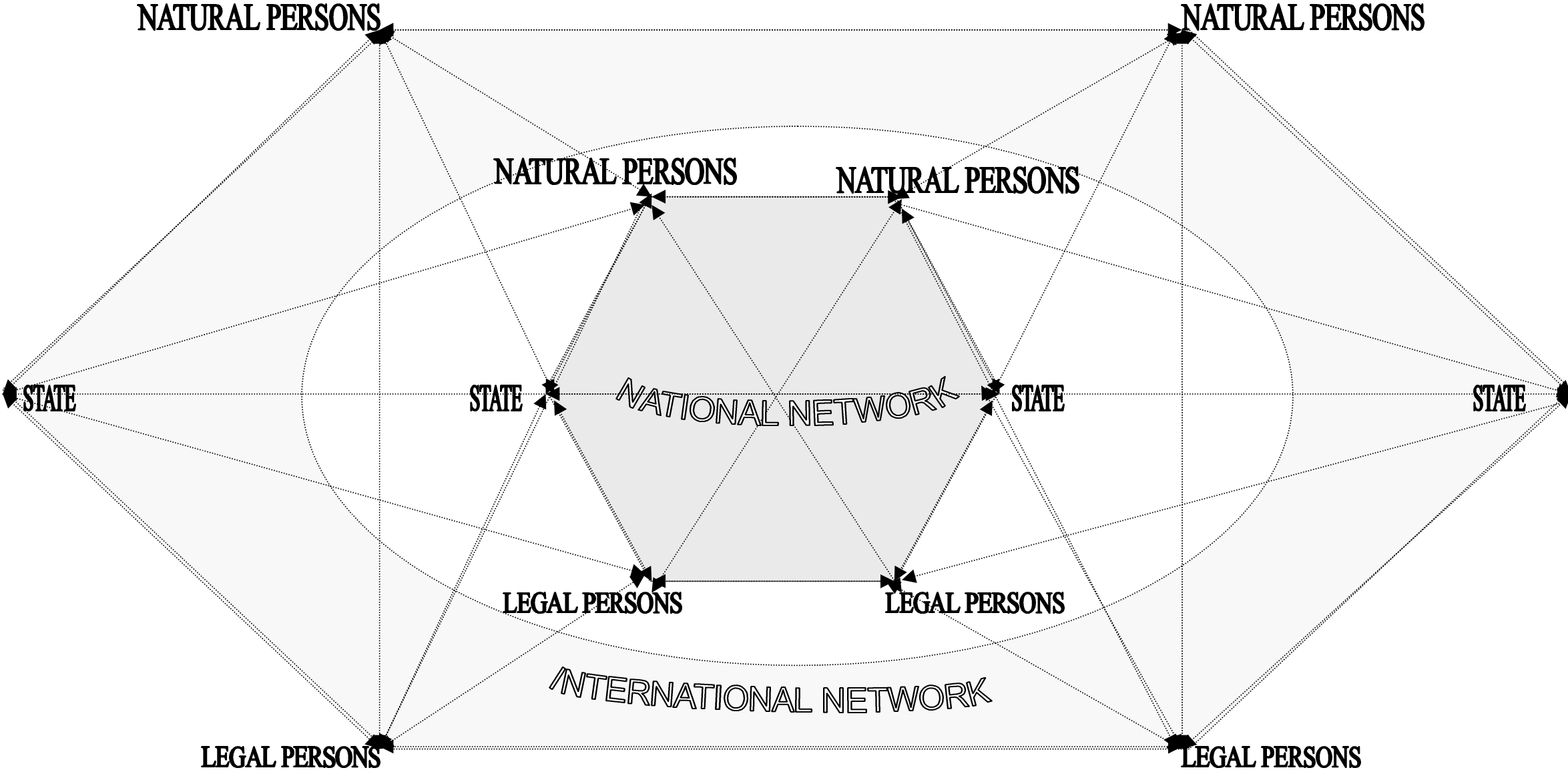
OF THE DOCUMENT



OF THE INFORMATION



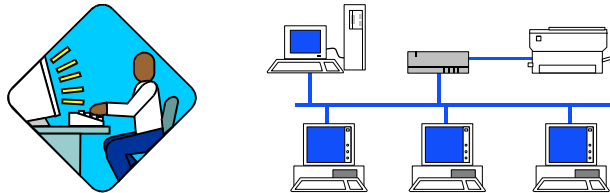
PERSONS AND THEIR INTERACTION



ASSIGNING A DOCUMENT TO A PERSON

WHY?

To establish a person's responsibility with respect to the document or the electronic vehicle used to transmit it and as evidence of a relation between the two






1. A document and a person or one or more electronic vehicles (author, consultant, person sending the document, etc.)
2. A document and two persons or one or more electronic vehicles (bilateral exchange of information, transaction or contract)
3. A document and several persons or one or more electronic vehicles (multilateral exchanges, contract between several persons)



HOW?

By various modes of assignment depending on the level of security required for each type of document

1. Access Code + journaling of access 
2. Personal identification code (PIN) + contract or predetermined agreement 
3. Institutionnal registration of persons, electronic vehicles and documents (data and metadata)
4. Signature of document, by hand or by electronic means in compliance with article 2827 of the Civil Code 
5. Combination of these modes, etc.

IDENTITY OF A PERSON IDENTIFIER OF AN OBJECT

OF WHOM?
OF WHAT?

ESTABLISHED
BY WHOM? BY WHAT?



OF PERSONS

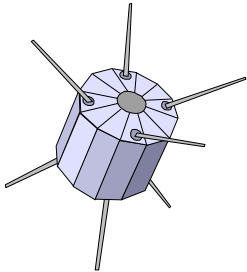
LEGAL EXISTENCE :
Evidenced by certificate of civil status (hard copy or electronic copy)



OF BUSINESSES
❖ Sole proprietorships
❖ Partnerships
❖ Companies

LEGAL EXISTENCE :
Evidenced by incorporating document, hard copy or electronic copy, filed with the Business Register

**PUBLIC
DOMAIN**



OF ELECTRONIC VEHICLES
1. Access servers
2. Links (optical fibers)

LEGAL EXISTENCE:
1, 2 and 3. Evidenced by the assignment of a distinguished name according to standards recorded in the Register of the person responsible for the vehicle or the object identified

**PUBLIC AND
PRIVATE
DOMAINS**



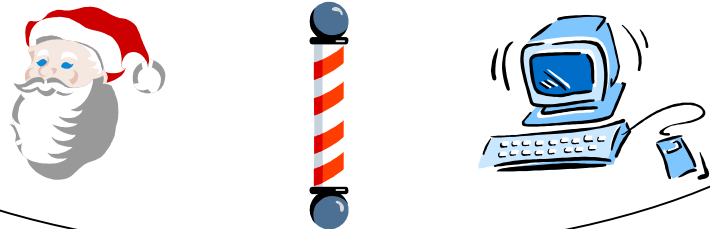
**OF INTERMEDIATE OBJECTS
OF COMMUNICATION :**
3. Public key certificates
4. Electronic documents

4. Evidenced by institutional registration

VERIFYING THE IDENTITY AND THE IDENTIFIER

**PUBLIC
OR
PRIVATE
DOMAIN**

1. The person, business or object whose identity or identifier needs to be verified possesses a **CHARACTERISTIC**



2. The person, business or object whose identity or identifier needs to be verified possesses or contains **KNOWLEDGE**



ANCHOR POINTS

3. The person, business or object whose identity or identifier needs to be verified possesses or contains an **OBJECT**



VARIOUS VERIFICATION METHODS:

Shape or biometrical measure:

- ❖ Fingerprints
- ❖ Iris
- ❖ Shape of the hand

Signature

Key, card, passport, other ID

VARIOUS VERIFICATION METHODS:

- Common name of a person
- Distinguished name of an object
- Identification number or code
- Algorithm or mathematical formula
- Hard copy or digital certificate
- Credentials
- Predetermined process
- Predetermined agreement

AUTHENTICATION = CONFIRMATION OF IDENTITY = RECOGNIZING SOMEONE OR SOMETHING

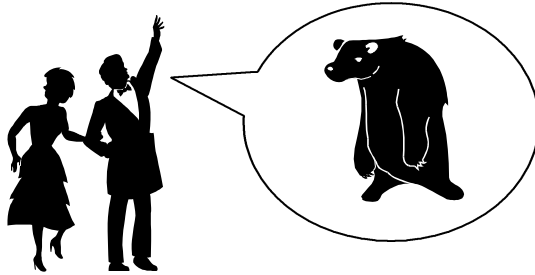
BY WHOM?

We depend on a person to recognize a person, a business or an object

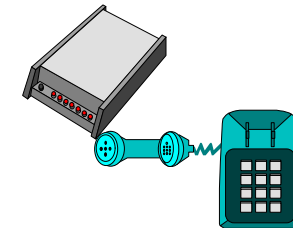
PUBLIC
OR
PRIVATE
DOMAIN

BY WHAT?

We depend on an object to recognize a person, a business or an object



ANCHOR POINTS



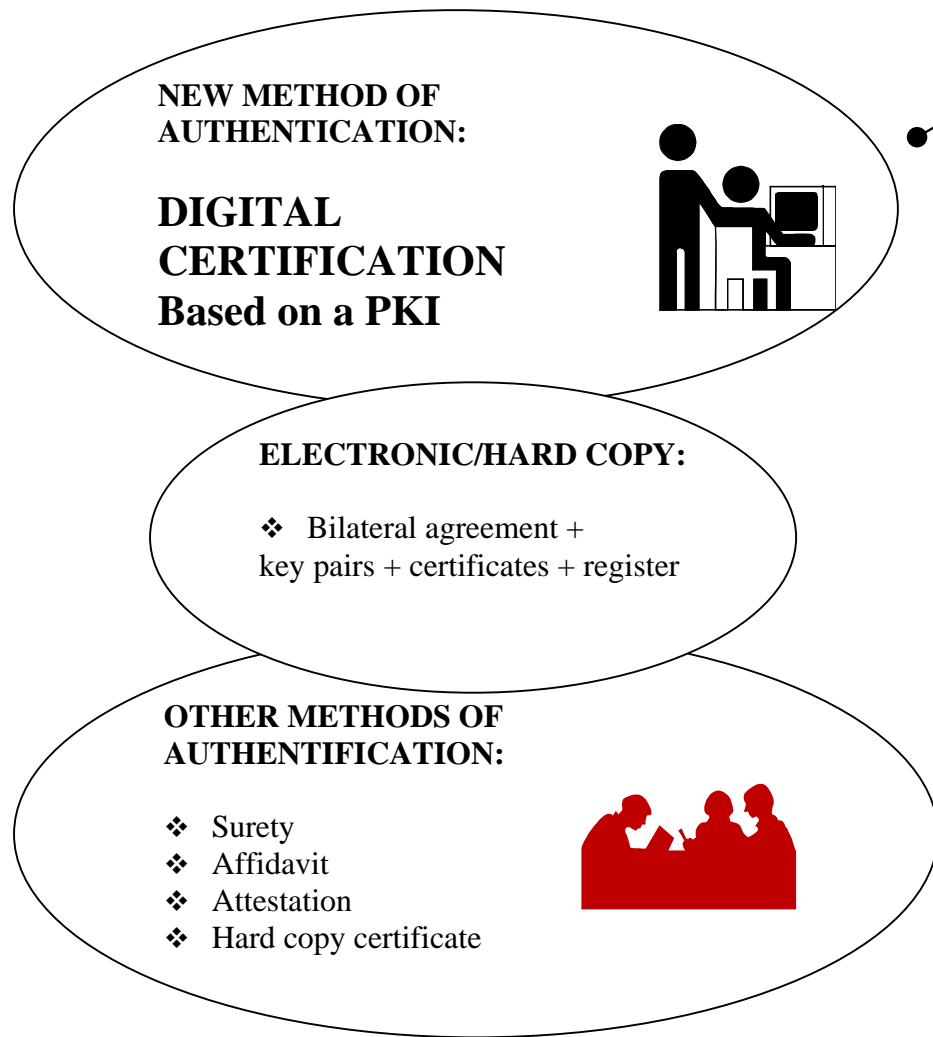
3. The person or object can recognize the **CHARACTERISTIC** of the person, business or object to be authenticated

1. The person has an **OBJECT** or the object contains another **OBJECT** through which to recognize the person, business or object to be authenticated

2. The person or object has the **KNOWLEDGE** required or can refer to someone or something in order to recognize the person, business or object to be authenticated

4. The person or object can **MATCH SEVERAL MEANS** of verifying the identity or identifier (e.g. physical characteristics + picture + physical presence)

METHODS OF AUTHENTICATION

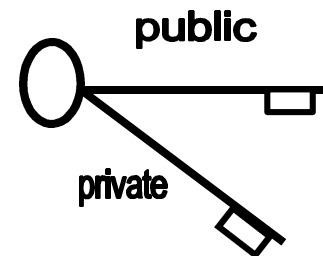


A PUBLIC KEY INFRASTRUCTURE (PKI)

FUNCTIONS:

DELIVERY AND MANAGEMENT

1. OF KEY PAIRS



2. OF CERTIFICATES



3. OF REGISTERS

of key pairs and certificates



CERTIFICATION

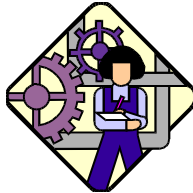
POSSIBLE CERTIFIERS IN THE PUBLIC AND PRIVATE DOMAINS

1. A **third party**:



- ❖ Notary
- ❖ Finance company
- ❖ Financial institution
- ❖ Specialized certification service

2. A **person in a position of authority** with respect to the person whose identity must be authenticated:



- ❖ An employer, for its employees
- ❖ A university, for its students
- ❖ A government, for its citizens

3. A **main party** in a transaction or a group:



- ❖ A large company, for its clients
- ❖

EXAMPLE :

The **GOVERNMENT**
could certify:

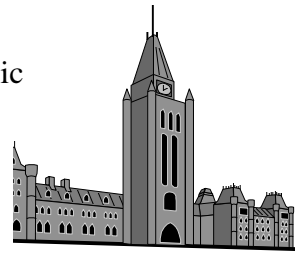
- ❖ Departments
- ❖ Agencies
- ❖ Department or agency employees
- ❖ Companies
- ❖ Partners
- ❖ Citizens dealing with the government



SHARING OF ROLES

LEGISLATOR :

The legislator defines the basic standards used to recognize the legal value of the document and the electronic exchanges.



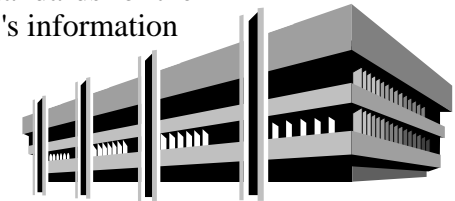
EXECUTIVE:

GOVERNMENT FUNCTION:

The government sets the standards for the implementation of Québec's information highway;

ADMINISTRATIVE FUNCTION :

The government fosters the implementation of the information highway and oversees its management.



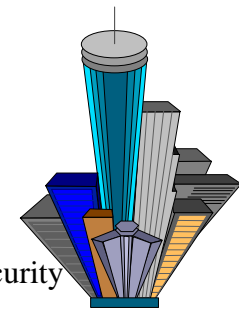
JUDICIARY:

The courts enforce the application of standards and adjudicate, in accordance with the rule of law, disputes concerning the rights and responsibilities of litigants with respect to electronic documents and vehicles.



PRIVATE SECTOR:

The private sector participates in the development and implementation of information technologies and the development of the technical standards required to guarantee the security of the information highway.



**STRUCTURE OF A
LAW
RESPECTING
SECURITY ON
THE
INFORMATION
HIGHWAY**

**INTRODUCE NEW
LEGAL NOTIONS
RESPECTING
DOCUMENTS,
IDENTIFICATION
OF PERSONS AND
LINKS BETWEEN
PERSONS
AND DOCUMENTS**

**PROVIDE FOR
ENABLING POWERS**

**ASSIGN DUTIES AND
RESPONSIBILITIES**

**MAKE NECESSARY
AMENDMENTS TO
ADAPT AND
HARMONIZE EXISTING
LEGISLATION**

EFFECT OF THE QUÉBEC LEGISLATION



| | |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>ENSURE COHERENCE IN THE LAW (CYBERSPACE = PAPERSPACE)</p> | <p>REFER TO TECHNOLOGICAL STANDARDS CONSISTENT WITH INTERNATIONALLY RECOGNIZED STANDARDS (ISO) (ITU) (IETF)</p> |
| <p>ENCOURAGE THE SIGNING OF AGREEMENTS WITH PARTNERS IN THE PRIVATE AND PUBLIC SECTORS TO ENSURE THE HARMONIZATION OF LEGAL SYSTEMS (MUTUAL RECOGNITION AGREEMENTS)</p> | <p>CONTRIBUTE, IN INTERNATIONAL FORUMS, TO THE ESTABLISHMENT OF INTERNATIONAL MODELS, STANDARDS OR CONVENTIONS (UNCITRAL) (OECD) (WIPO)</p> |



THE VISION FOR THE FUTURE



A GLOBAL VISION