Consortium meeting
"InfoCities" in Antwerpen & Liège on 19th to 21 October 1998

Information security
&
Electronic Commerce

See also:
http://www.titan.be

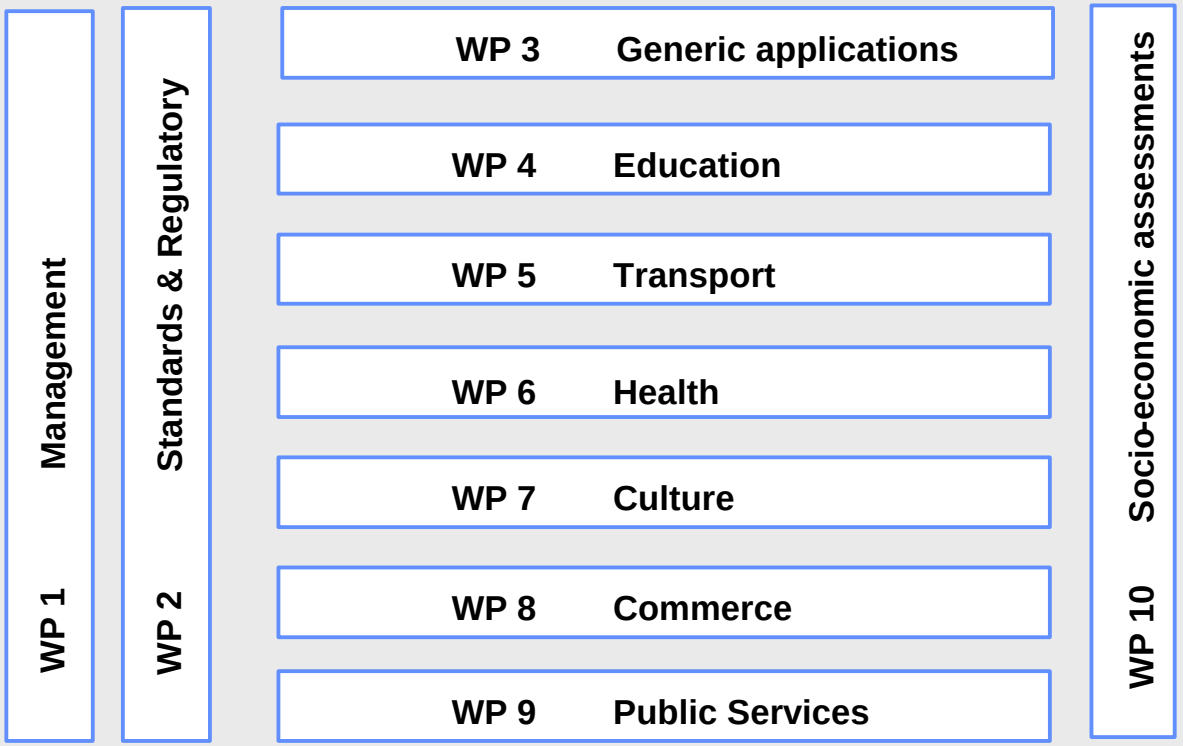
Prepared by: Guy Maréchal
Senior adviser Information Security & Multimedia
Tel / Fax : + 32 2 648 98 28
E-Mail: g.marechal@skynet.be

Consortium meeting
"InfoCities" in Antwerpen & Liège on 19th to 21 October 1998

Information security
&
Electronic Commerce

• Introduction to the Information security	by Guy Maréchal (PROSI)
• The methods, standards & tools of the E-Commerce	by Philippe Bellens (Banksys)
• The legal aspects of the E-Commerce	by Severine Dusollier (CRID)
• Questions & answers	all member & panel

Prepared by: **Guy Maréchal**
Senior adviser Information Security & Multimedia
Tel / Fax : + 32 2 648 98 28
E-Mail: g.marechal@skynet.be



General Work Package structure of the InfoCities project

(feasibility phase)

Definitions

- **INFORMATION :**

  The meaning that human assigns by means of conventions (formats) applied to the data.

- **DATA :**

  A representation of facts, concepts or instructions in a formalized (§) manner suitable for communication, interpretation or processing by human, or by automatic means.

- **DOCUMENT :**

  Data represented on a spatial (§) storage medium.

- **MESSAGE :**

  Data represented on a temporal (§) storage medium. By extension, a Document transmitted (possibly with replication) from a sender to an addressee.

- **EVIDENT Document :**

  Document that human could acquire its information without any use of non-genuine tools

- **DEMATERIALIZED Document :**

  A document that human could acquire its information only though use of non-genuine tools

- **AUTO-CONCLUSIVE Document :**

  A document that human could be convinced of its integrity from its included data.

- **ORIGINAL Document :**

  A document in which the data are bind on the carrier on which they have been created.

(§) Format; Place & Moments

Democratic Principles

- **The Functional approach :**

  A framework must be found, established and used by the public authorities, private moral & physical persons to encompass information handling (telecommunication, processing, storage and human interaction) & activation (Computer Integrated Manufacturing, …) with
  - the same functions and contents as those currently on offer for local non dematerialized human actions and interactions and
  - the new functions and contents of the Information Society as those exploiting its specific novelties.

- **The Open Context :**

  The Society should be organized in such a way that the regulatory framework is no more restrictive than necessary for the correct operations of the society and sufficiently open to permit the values, rights, responsibilities and duties of everyone to be respected and promoted.

- **The Regulatory fitting means :**

  The Society should be organized in such a way that the tools, equipment and infrastructures implement "a priori" the right way of acting & interacting, in such a way that spontaneously, by construction, everybody would do right according to the law, standards, forms, ... , so with minimum enforcement required. Without that the dominant "Country" will force its laws and values through its techniques !!!

- **The Public Interest :**

  The Public authorities should promote the Information Society assets, use them and interact accordingly with the Citizen. In particular, contents is not a good like others !

Information Security for Documents & Messages
(identify functions of the domain)

- **The Information security functions :**
  - Integrity (no changes, unless intended & authorized)
  - Authenticity of the actors implementing roles (no ambiguity on who is who)
  - Bundling of Integrity & Authenticity (Signature)
  - Balance Security-Risks-Form (Behavior, Prevention, Detection, contention, Reactions)
  - Non repudiation (assurance that the involved actors could not deny their involvement)
  - Singularity (assurance that only one use is possible at one moment)
  - Conformity (assurance that the format(s) used in the document is (are) conformed to their definition, as to allow the understanding of the data, as "Information")
- **The Information security functions in their context :**
  - Hiding (no-one except the involved knows the existence of the document)
  - Anonymity (no-one except the involved knows the identity of the involved actors)
  - Confidentiality (no-one except the involved knows the contents of the document)
  - Tracing (the involvement of the actors is traced)
  - Life cycle control (including failure recovery)
- **The Information security functions for the DEMOCRATIC access :**

  The democratic access to documents and messages consists in the assurance given to the public authorities that they will have the possibility (as an exception; when allowed or imposed by law; under democratic control) to know the existence, the identity of the actors, the contents of a document or its tracing.

Information Security for Documents & Messages

(identify functions of the new formal ways; create a new environment)

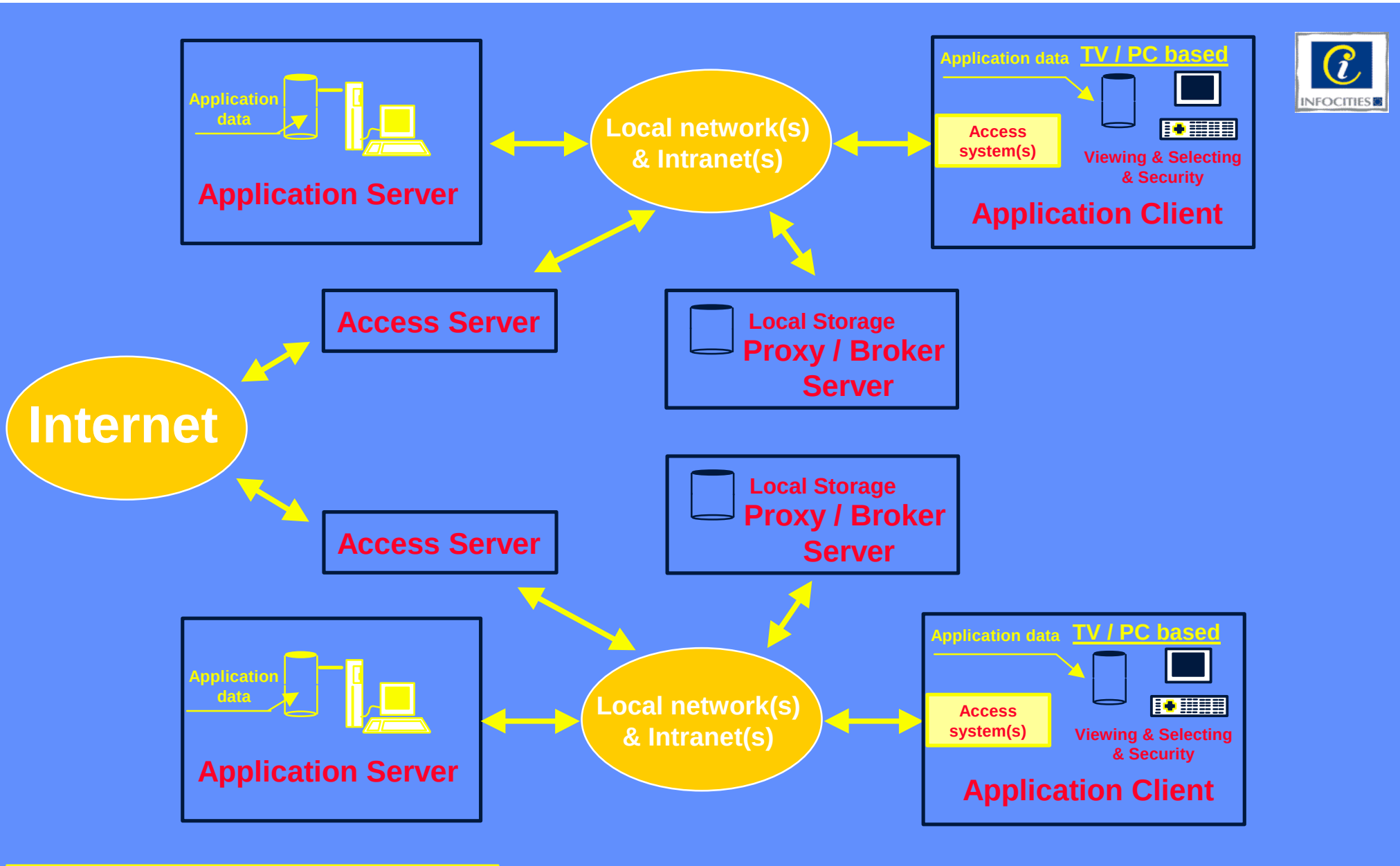
- **The digital signature :**
  - The use of the digital signature should be allowed & framed by LAW
  - The format allowed should be specified
  - The Application & Quality criteria should be given
  - The Accreditation criteria of the required quality should be established (under state control)
- **The Public authorities :**
  - The Roles and Actors should be identified and defined under state control
    - The physical persons
    - The moral persons
    - The power of mandate for roles
  - The dynamic control of the existence and legal power of the actors should be in the hands of the public authorities
  - The Accreditation of the Trusted Third Parties
  - The Formats & Labeling control (Understandability; Intellectual rights ownership & responsibility)
- **The Trusted Third Parties :**

  The Trusted Third Parties which are not required to be in hands of the public authorities should be accredited (Time stamp; certified archiving; certified brokerage, …)
- **The Democratic monitoring :**

  The democratic monitoring should be organized in such a way that it would be impossible for the Public Authorities to do things that are not conform to the Law and it would be possible to monitor in a real democratic way.

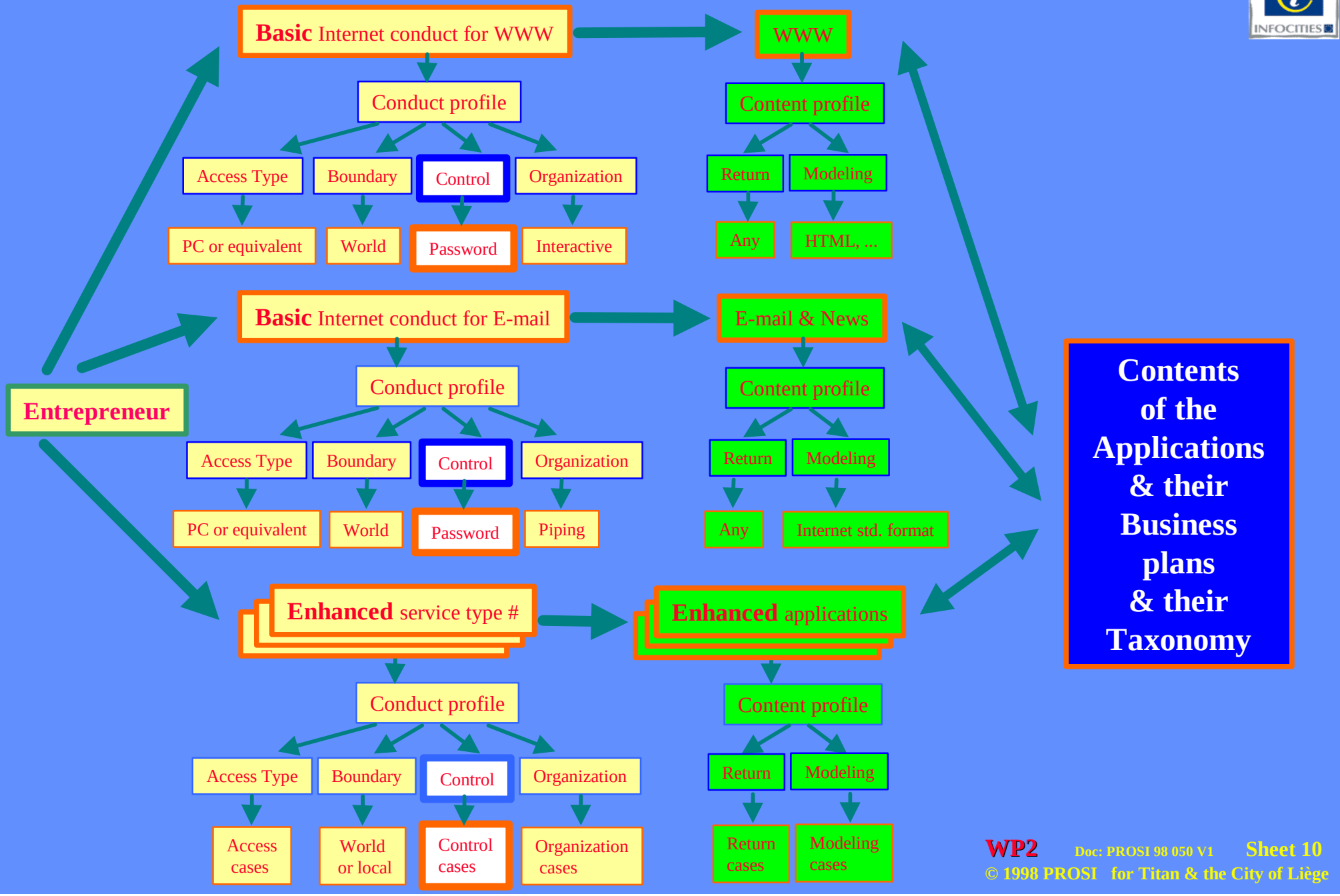
The Coding of the Information security controls

Layer 5 (Content data):	Naming of actors; certificates
Layer 4 (Service & access data):	Key values; labeling;
Layer 3 (Access system):	Internet addressing; C-SET
Layer 2 (Network):	TCP-IP security controls
Layer 1 (Carrier):	Smart cards



General CONFIGURATION
for Internet on Hybrid networks
(Many cases, in particular Case §§)

General Technical Taxonomy



Consortium meeting
"InfoCities" in Antwerpen & Liège on 19th to 21 October 1998

Information security
&
Electronic Commerce

• Introduction to the Information security	by Guy Maréchal (PROSI)
• The methods, standards & tools of the E-Commerce	by Philippe Bellens (Banksys)
• The legal aspects of the E-Commerce	by Severine Dusollier (CRID)
• Questions & answers	all member & panel

Prepared by: **Guy Maréchal**
Senior adviser Information Security & Multimedia
Tel / Fax : + 32 2 648 98 28
E-Mail: g.marechal@skynet.be