

ISACA Round Table

BISI – Norm track



General information
Objectives
Actual situation



Ir. Alain De Greve, MCA, CISA

28/10/2009

ir. Alain De Greve

1

Norm track (extract whitepaper of September 2008)



- Minimal information and ICT security requirements based on international standards [see Annex C] should be specified and fully integrated into the various industry sector regulations. These should deal with aspects such as information security management and control framework, risk management, incident management, business continuity, evaluation and audit, reporting and compliance, etc. The requirements should also mention the need for accreditation for critical systems. The administration should lead the way for industries and private organizations where accreditation is not part of the implementation of security solutions.

- A number of information security standards allow for evaluation/certification. Currently Belgian manufacturers and organizations need to go abroad for the certification of their information security products and services. In view of the increasing professionalism in the sector and the increased demand for certified products and services, Belgium should establish its own information security certification framework, based on international standards in accordance with Belgian law and regulations. In this case the Belgian Accreditation Body (BELAC) should accredit the required information security certification authority and any evaluation center's). This governmental information security certification authority would then be in a position to issue the required certified products and services.

The initiative already begun in this area should continue to receive the necessary support in order to achieve these objectives.

The accredited information security certification organization should collaborate with other national certification bodies within the EU through the Common Criteria Recognition Agreement [7]. The aim would be to establish a harmonious certification framework with the other member states for the translation of standards enforced through European directives into the national certification program. On a larger scale (worldwide) this body needs to establish frameworks with peer organizations for cross-certification.

- Belgian efforts in international information security standardization need to be better coordinated. Although excellent work is being delivered by Belgian experts in these forums, there is no support or recognition from the Belgian Standardization Office (NBN). This coordinating role could, for instance, be fulfilled by Agoria, by acting as a single point of contact for the ICT sector ("sector operator"). These coordinated activities should be supervised by the Ministry of Economic Affairs and the Department of Scientific Policy.

28/10/2009

ir. Alain De Greve

2

Three Sub – objectives (01)



- Sub-01 : Information Security Norms of interest for Belgium and Belgian's
 - Establish a list of international norms from all kind of origins with a potential interest for citizen and governments
 - Try to find priorities in the forest for synergies
- Sub-02: Put in place a “Belgian Scheme” for certification of products, services and systems
 - Identify the aspects regarding information security related certifications (e.g. Common Criteria, ITIL, 27001,...)
 - Look at the Belgian expectations, the actual situation, collaborate with neighborhood countries to identify best practice and potential synergies and finally ensure independence of Belgium for recognized national strategic sectors, critical infrastructures,...
- Sub-03: Ensure Belgian delegation at international level
 - Ensure presence and contacts of recognized Belgian expert's in international forum and organizations (CEN, ETSI, ISO, ITSMF, ECSCA,...) with as a result a greater visibility for the Belgian community
 - Identify what exists worldwide and where we should put our interest for the public and private Belgian sector
- Phased approach

28/10/2009

ir. Alain De Greve

3

BISI objective: 1 > Activities



- Inventory of the committees with a representative identified in Belgium
- Mailing to other committees to see the level of activity
- See the situation and look for potential synergies
- Setting up an inventory scheme to categorize the importance/relevance of these norms

- Based on the ENISA personally activity related to the WG on RM/RA inventory

Suffer some delay

—

lack of resources and insolvent of participants

28/10/2009

ir. Alain De Greve

4

The different actors in the norm sector



World level

Regional level

Country level



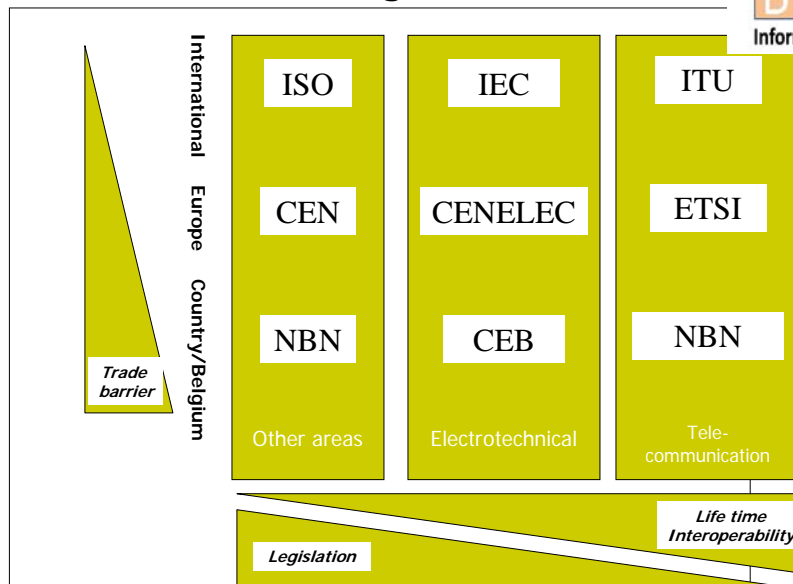
28/10/2009

ir. Alain De Greve

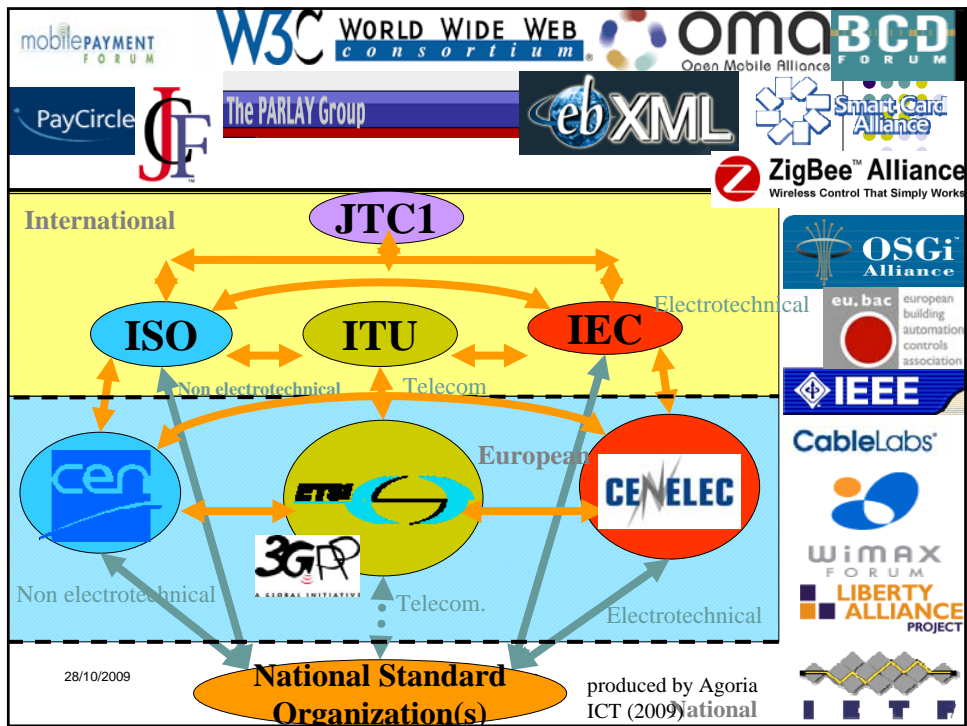
5

Standardization organizations

produced by Agoria ICT(2009)



6



Non exhaustive list of potential IT Security related norms (under investigation)

- Only ISO level:
- JTC 1/SC 17 : cards and personal identification
 - JTC 1/SC 27 : IT Security Techniques
 - JTC 1/SC 31 : Automatic identification and data capture techniques
 - JTC 1/SC 37 : biometrics
 - TC 8 : Ships and marine technology
 - TC 20 : Aircraft and space vehicles
 - TC 21 : Equipment for fire productin and fire fighting
 - TC 22 : Road vehicles
 - TC 28 : Petroleum products and lubricants
 - TC 34 : Food products
 - TC 58 : Gas cylinders
 - TC 67 : Materials ,equipment and offshore strcures for petroleum ,petrochemical and natural gas industries
 - TC 68/SC 2 : Security management and general banking operations
 - TC 68/SC 6 : retail financial services
 - TC 76 : Transfusion , infusion and injection equipment for medical and pharmaceutical use
 - TC 85 : Nuclear enery
 - TC 92 : Fire safety
 - TC 94 : Personal safety – protective clothing and equipment
 - TC 98 : Bases for design of structures
 - TC 104 : Freight containers
 - TC 122 : Packaging
 - TC 145 : Graphical symbols
 - TC 146 : Air quality
 - TC 147 : Water quality
 - TC 154 : Processes, data elements and documents in commerce ,industry and administration
 - TC 159 : Ergonomics
 - TC 162 : Doors and windows
 - TC 184 : Industrial automation systems and integration
 - TC 190 : Soil quality
 - TC 192 : Gas turbines
 - TC 197 : Hydrogen technologies
 - TC 204 : Intelligent transport systems
 - TC 211 : Geographic information/Geomantic
 - TC 212 : Clinical laboratory tesing and in vitro diagnostic test systems
 - TC 215 : Health informatics
 - TC 220 : Cryogenic vessels
 - TC 223 : Civil defence
 - TC 224 : Services activities relating to drinking water supply systems and wastewater systems – Quality criteria of the service and performance indicators
- 28/10/2009



To be added :
Some other
organizations
and federations

Three Sub – objectives (02)



- Sub-01 : Information Security Norms of interest for Belgium and Belgian's
 - Establish a list of international norms from all kind of origins with a potential interest for citizen and governments
 - Try to find priorities in the forest
- Sub-02: Put in place a “Belgian Scheme” for certification of products, services and systems
 - Identify the aspects regarding information security related certifications (e.g. Common Criteria, ITIL, 27001,...)
 - Look at the Belgian expectations, the actual situation, collaborate with neighborhood countries to identify best practice and potential synergies and finally ensure independence of Belgium for recognized national strategic sectors, critical infrastructures,...
- Sub-03: Ensure Belgian delegation at international level
 - Ensure presence and contacts of recognized Belgian expert's in international forum and organizations (CEN, ETSI, ISO, ITSMF, ECSA,...) with as a result a greater visibility for the Belgian community
 - Identify what exists worldwide and where we should put our interest for the public and private Belgian sector
- Phased approach due to the large scope
 - Contacts with some organizations like Agoria, Fedict, ANS

28/10/2009

ir. Alain De Greve

9

BISI objective: 2 > certification scheme



- Inventory of needs
 - Advantages
 - Problems
 - Persons
 - Systems
 - Products
 - Entities
- Priority on C. C.
 - First « dry run » succeeded recently
 - Close collaboration with Cetic and some administration departments (Belac / ANS)
 - Look for next steps in order to finalize a Belgian independence in critical domains

Seems on the good way

—
Priorities defined, no specific delay

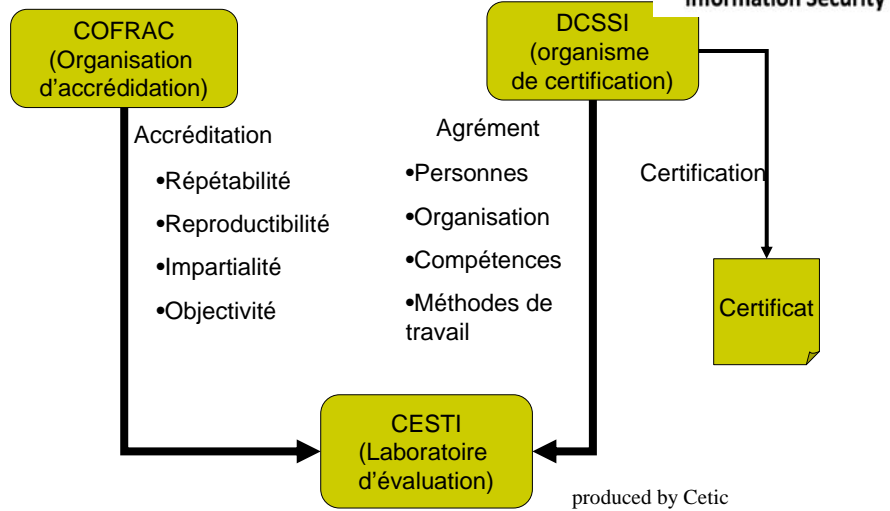
On persons and systems/entities already also ongoing

28/10/2009

ir. Alain De Greve

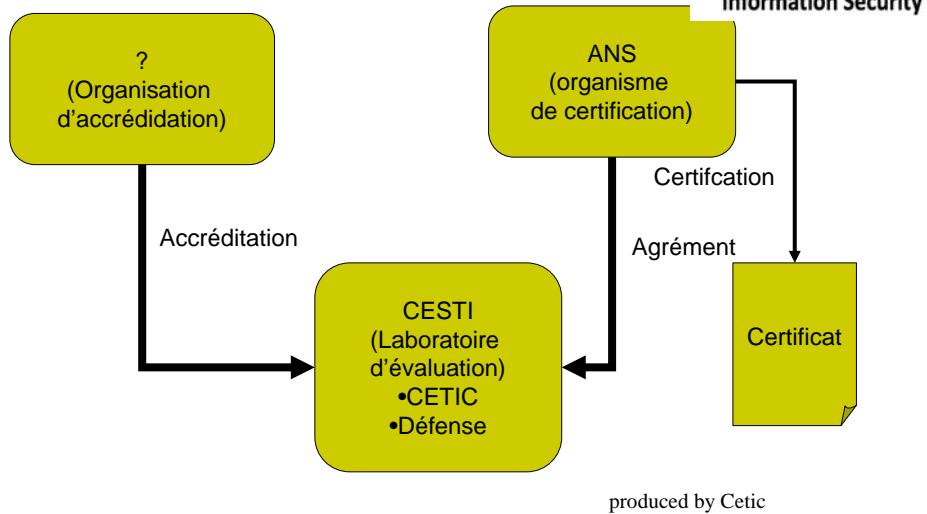
10

French Scheme (C.C.)



11

Belgian scheme under development



12

Scope in Belgium



- Both sectors
 - Public
 - Private

- When
 - Handling of classified information in computer information system

- What is ongoing
 - Adaptation of the law, KB , ("cadre juridique")
 - Some ANS/NVO publication
 - Instructie INFOSEC ,homologatie-strategie , versie 1.0

- Four groups for national technical norm
 - KUL – UCLLN
 - Standards and parameters
 - Mathematical evaluation
 - Secure implementation
 - Certification agency and Common Criteria

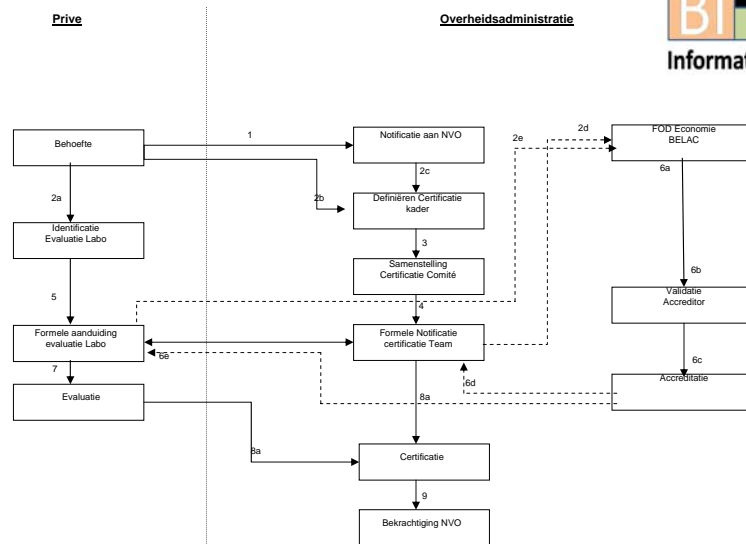
- C.C.R.A.
 - Still awaiting government

28/10/2009

ir. Alain De Greve

13

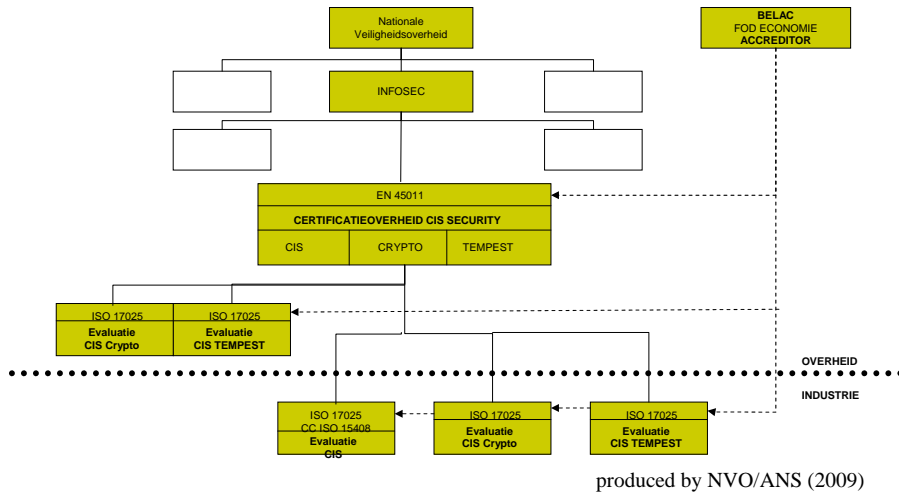
Two ways to reach certification : intermediary solution



produced by NVO/ANS (2009)

14

Two ways : final solution



15

First step – Dry run



- This draft schema has been played :
 - ETCA (Product of Thales)
 - ANS – Certification authority
 - Cooperation « Defence » - CETIC - CESTI
 - *approval certificate* but not certification
- Business Case
 - Security Target written by Thales evaluated by CETIC and Defence
 - ANS has awarded a certificate of approval
- Not certification → Thus not official at international level

- Next steps in the hands of government (international recognition – CCRA)
 - Belgian complexity , but on the good way
- Classification of information , minimal requirements for some circumstances

produced by Cetic (2009)

28/10/2009

ir. Alain De Greve

16

Three Sub – objectives (03)



- Sub-01 : Information Security Norms of interest for Belgium and Belgian's
 - Establish a list of international norms from all kind of origins with a potential interest for citizen and governments
 - Try to find priorities in the forest
- Sub-02: Put in place a “Belgian Scheme” for certification of products, services and systems
 - Identify the aspects regarding information security related certifications (e.g. Common Criteria, ITIL, 27001,...)
 - Look at the Belgian expectations, the actual situation, collaborate with neighborhood countries to identify best practice and potential synergies and finally ensure independence of Belgium for recognized national strategic sectors, critical infrastructures,...
- Sub-03: Ensure Belgian delegation at international level
 - Ensure presence and contacts of recognized Belgian expert's in international forum and organizations (CEN, ETSI, ISO, ITSMF, ECSA,...) with as a result a greater visibility for the Belgian community
 - Identify what exists worldwide and where we should put our interest for the public and private Belgian sector
- Phased approach

28/10/2009

ir. Alain De Greve

17

BISI objective: 3 > international support and representation



- Look for needs
 - Priority
 - Resources
 - Points of interest
- ISO ←-
- NIST
- BSI
- CEN ←-
- ITU ←-
-
- ←- For collaborating in some committee don't hesitate to contact me or Agoria ICT
- Quite large a scope
 - Step by step approach
 - Support and publicity
 - Control of what is currently done individually
- Role of national institutions (e.g. NBN)
 - Next context with new law
 - Agoria ICT as sector operator plays an active role in this domain helping actually at logistical level

28/10/2009

ir. Alain De Greve

18

Other Groups



- Belgian host CEN and CENELEC
 - International meeting – workshop regularly

Seventh CEN StandardDays

Open info days on European Standardization
 27- 28 October 2009
 CEN-CENELEC Meeting Centre, Brussels

> Programme Day 1	> Registration
> Programme Day 2	> Venue & accomodation

- ETSI
 - International workshop foreseen end of January in south of France



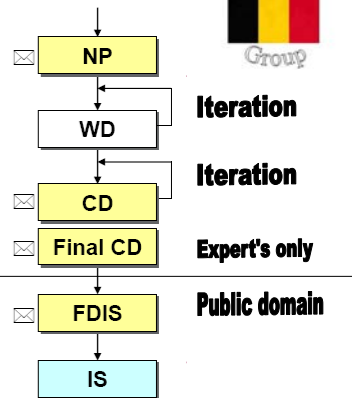
28/10/2009

ISO Norm Production Schema (standard)



Maturity level / state of standardization

- Study Period / New Project (NP)
 - 2 month NP letter ballot*)
- Working Draft (WD)
- Committee Draft (CD/FCD)
 - 3 month CD ballot(s)
 - 4 month FCD ballot
- Draft International Standard (DIS/FDIS)
 - 2 month FDIS ballot
 - no more comments at this stage
- International Standard (IS)
 - review every 5 years
 - or after 'defect report'

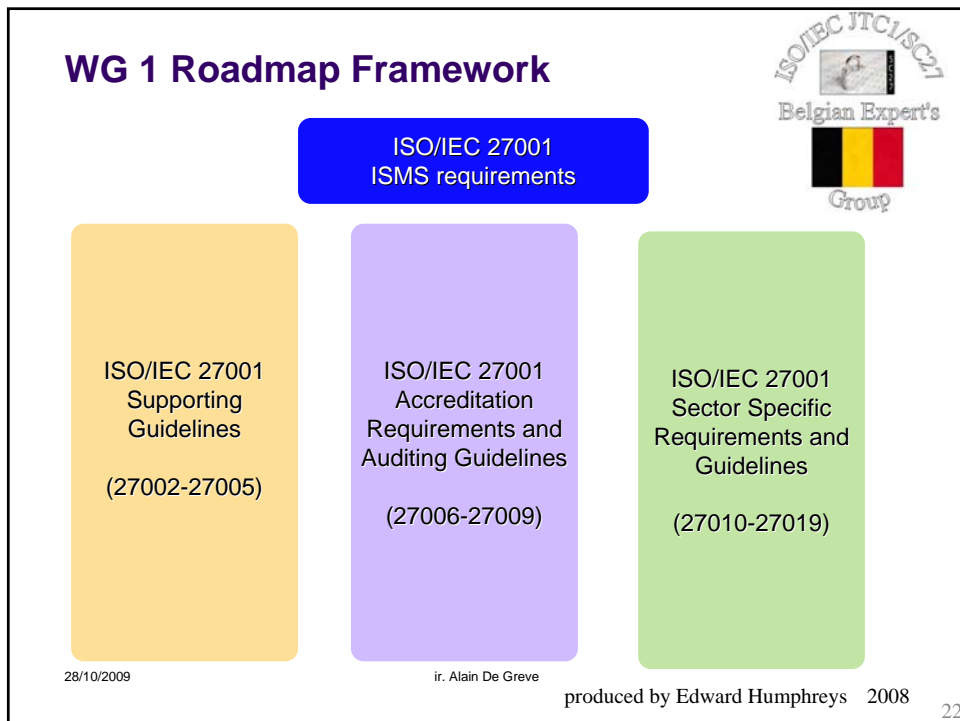
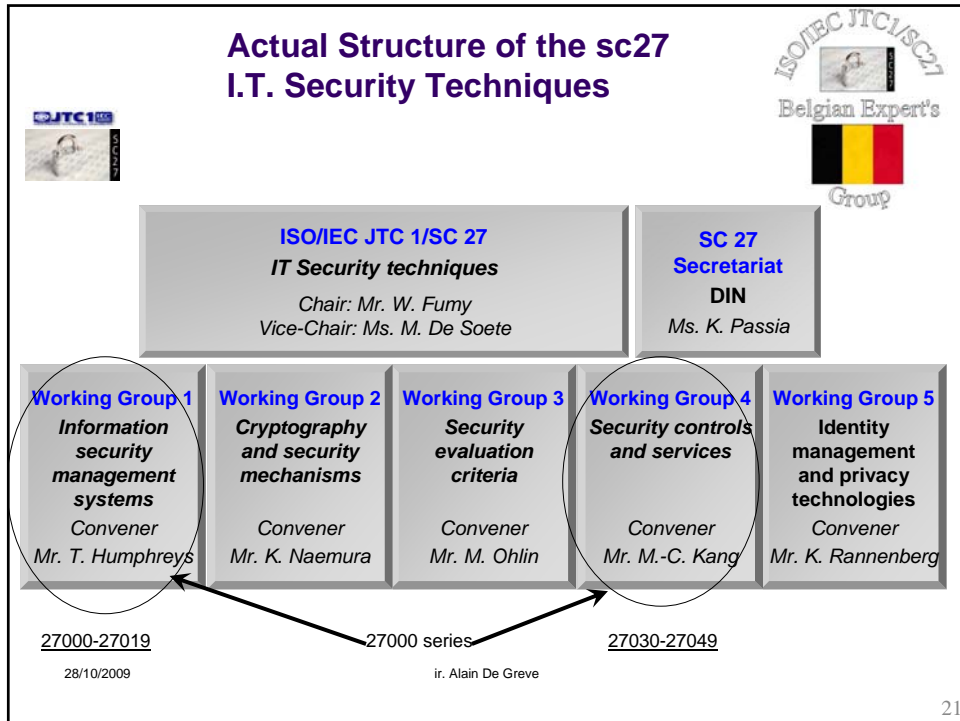


*) one vote per P-member

Thus normally actually around 2.8 years

28/10/2009

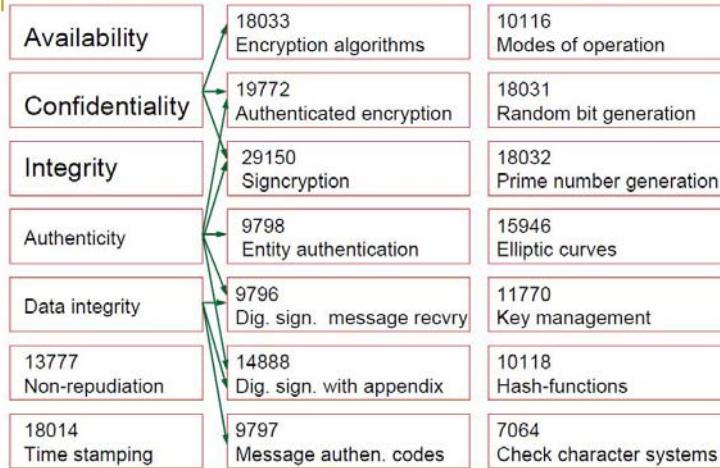
ir. Alain De Greve



WG 2 Roadmap Framework



Goals, Techniques, Mechanism and Algorithms



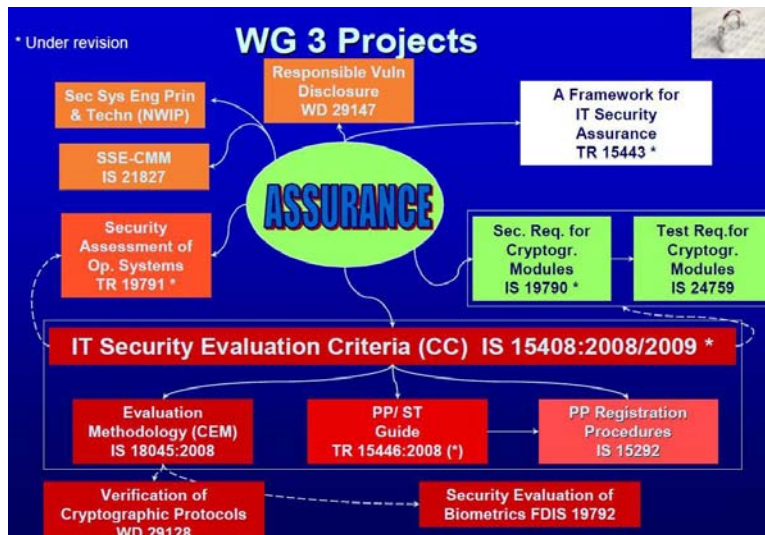
28/10/2009

ir. Alain De Greve

produced by K. Naemura 2008

23

WG 3 Roadmap Framework



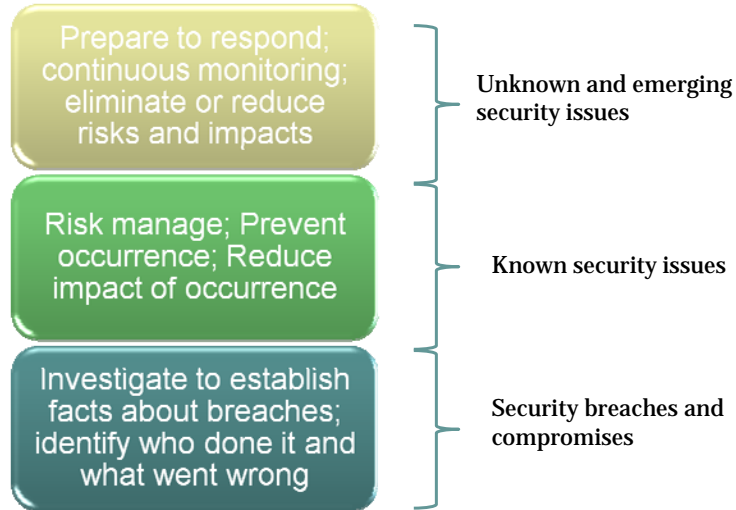
28/10/2009

ir. Alain De Greve

produced by M. Ohlin 2008

24

WG 4 Roadmap Framework



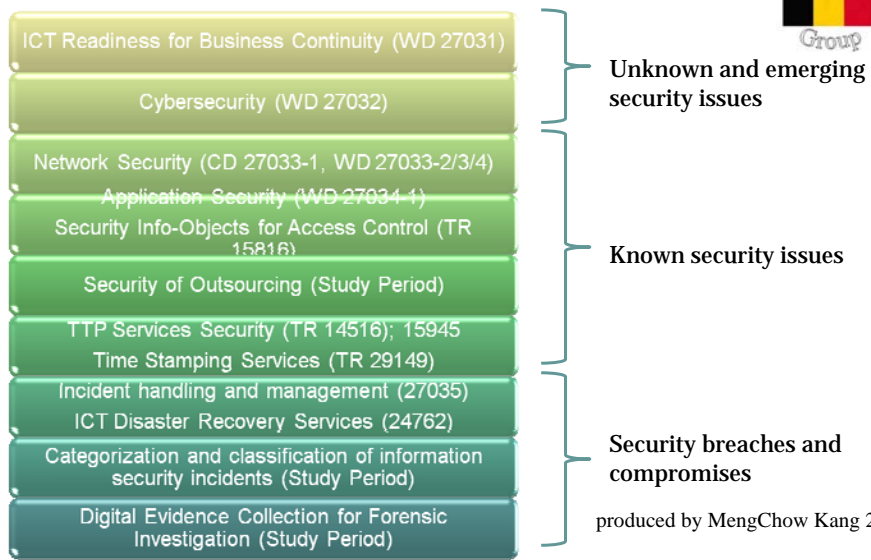
28/10/2009

ir. Alain De Greve

produced by MengChow Kang 2008

25

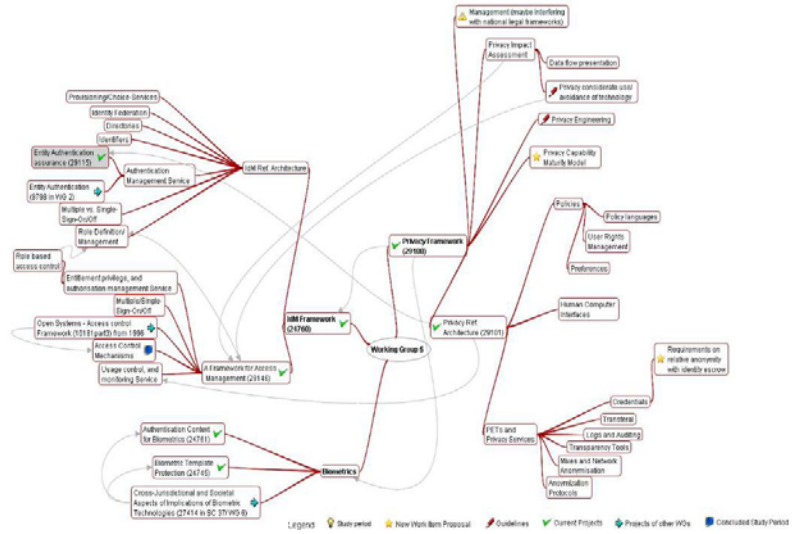
WG 4 Projects & Study Periods



produced by MengChow Kang 2008

26

WG 5 Roadmap Framework



28/10/2009

ir. Alain De Greve

produced by Kai Rannenberg 2008

27

Coming events

- Main issues
 - Budget
 - Empowerment
 - Resources
- Next meeting:
 - Before X-mas in December
- Spring 2010
 - Presence and presentation at Infosecurity.be
- Meetings are held at "Diamant Conference Center" (Agoria ICT building)
- Take a look at www.ictstandards.be for more details



28/10/2009

ir. Alain De Greve

28



Q & A

For further information

•E-mail :

•alain.degreve@skynet.be

28/10/2009

ir. Alain De Greve