Formation TLS-SEC – 5èmes Années

deux séances en janvier 2018 (secteur SANTÉ)

Module de cours

"aspects organisationnels de la sécurité des systèmes d'information"

Volet du module de cours

"introductions : audit / management / bonnes pratiques / analyse de risques"

- ***A.C.C.E.S.S.S.-I.F.***
  Audit / ***C***onseil / ***C***onsulting / ***E***xpertise en ***S***écurité / ***S***ûreté / ***S***ouveraineté des ***I***nformations et des ***F***onctions
- **Intervenant :**
  M. Gilles TROUESSIN
  gilles.trouessin@orange.fr
  Tél: +33 (0)6.63.10.50.76

Plan de cours (extraits)

Extraits des séances de cours suivantes :

- Aspects « généralistes » de la sécurité des systèmes d'information
- Aspects « appliqués » de la sécurité des systèmes d'information
- Aspects « sectoriels » de la sécurité des S.I. de la sphère santé/social
- Aspects « normatifs » pour aider la en œuvre de la sécurité des S.I.
- Aspects « analyse de risques » en sécurité de l'information

Objectifs pédagogiques proposés pour le domaine SANTÉ :

- Généralités des démarches liées à la sécurisation
- Besoins objectifs et exigences de sécurisation
- Propriétés et robustesse de la sécurisation
- Applications pratiques de la sécurisation
- Adaptation sectorielle de la sécurité

Fils conducteurs

Fil conducteur terminologique :

- De la *Sûreté de fonctionnement* à la dimension *Sécurité-Security*
- De la *Sécurité-Security* aux deux définitions de la *Confidentialité*
- De la garantie de *Confidentialité* au respect de la *Vie privée-Privacy*
- De la *Vie privée* à la protection des données à caractère personnel
- De la protection de données personnelles au projet d'anonymisation

Fil conducteur méthodologique :

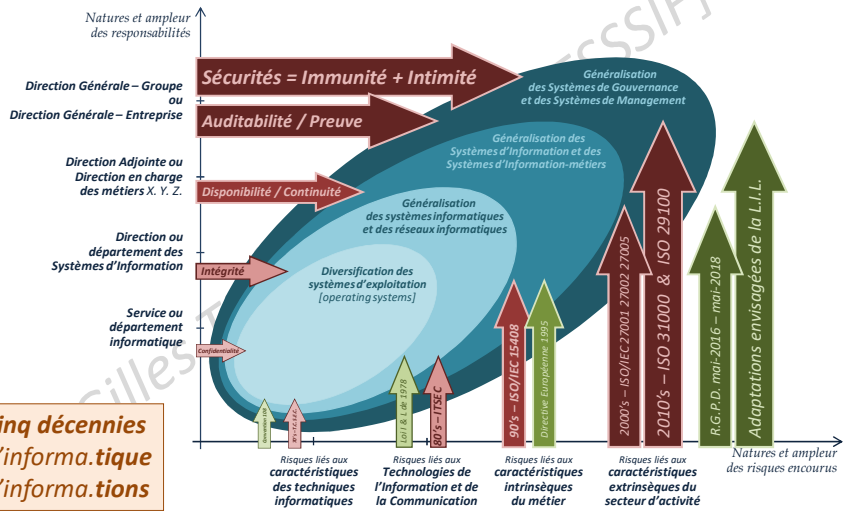
- Généralités sur les aspects organisationnels de la SSI
- Généralités sur des applications sectorielles de la SSI
- Illustration sur des démarches-projet de type PCA/PRA
- Présentation du management en matière de SSI (ISO27001)
- Présentation des bonnes pratiques pour la SSI (ISO27002)
- Présentation de l'analyse de risques en SSI (ISO27005)

 gilles.trouessin@orange.fr +33 (0)6.63.10.50.76

Journée régionale *R.G.P.D.* et *P.M.E.*

Réflexions académiques & Partages d'expériences

Université Toulouse I – Capitole & Master2 – Droit & Numérique



Cinq décennies d'informa.tique d'informa.tions

 4

PHASE-1 – PRÉSENTATION

Étape-1 – Terminologie & définitions

terminologie, définitions, solutions, perspectives, etc.

Qu'est-ce que la *Sûreté de Fonctionnement ?*

Sûreté de fonctionnement / …

La *"sûreté de fonctionnement"* d'un système informatique est la *"**propriété générique** qui permet aux utilisateurs de placer une **confiance justifiée** dans le service délivré par le système [Laprie88]"* :

- ✓ L'intégrité _____ vis-à-vis de la non-occurrence *"de modifications inadéquates"*
- ✓ La fiabilité _____ vis-à-vis de sa capacité à offrir une *"continuité de service"*
- ✓ La disponibilité _____ vis-à-vis de son aptitude à *"être toujours prêt à l'usage"*
- ✓ La confidentialité _____ vis-à-vis de l'absence *"de divulgations inappropriées"*
- ✓ La *"maintenabilité"* _____ vis-à-vis de sa capacité *"à être réparer et à évoluer"*
- ✓ La sécurité-innocuité _____ vis-à-vis *"des défaillances dites catastrophiques"*

Incluant donc :

- ➢ La sécurité-immunité _____ vis-à-vis de la *"protection des informations manipulées'* ou sécurité-*security*

Qu'est-ce que la *Sécurité du Système d'Information?*

Sûreté / sécurité / …

La *"sécurité (du S.I.)"* ou *Sécurité-Security* est la combinaison des *"**propriétés de base** qui (si elles sont fournies) permettent de **garantir que** les informations sont manipulées **de façon autorisée**".*

On parle de plus en plus de DICA :

- ✓ La **D**isponibilité_____pas de *"rétention/blocage"* non autorisée de l'information
- ✓ L' **I**ntégrité_____pas de *"modification/altération"* non autorisée de l'information
- ✓ La **C**onfidentialité___pas de *"divulgation/propagation"* non autorisée de l'information

Avec aussi et surtout :

- ➢ L' **A**uditabilité©_____ *"capacité du système à auditer"* le(s) élément(s) mis en œuvre et *"capacité du système à auditer"* la(les) sécurité(s) mis(es) en place

Autrement dit :

_____ *"capacité à fournir les preuves de la confiance"*

points de contrôles utiles (traçabilité/imputabilité) et utilisables (opposabilité/irréfutabilité)

 gilles.trouessin@orange.fr +33 (0)6.63.10.50.76

Qu'est-ce que la *Confidentialité ?*

Sûreté / sécurité / confidentialité / …

La *"confidentialité"* est cette *"propriété qui permet de garantir que les informations sont divulguées de façon autorisée"* :

- ➢ Confidentialité_____accès à l'information en justifiant du *"besoin d'en connaître"*
- ➢ Secret "médical"_____accès légitime mais dans le respect du *"colloque singulier"*
- ➢ Secret professionnel_____accès autorisé à l'information mais *"obligation de réserve"*
- ➢ Discrétion professionnelle_____accès inévitable avec obligation de *"respect de l'individu"*

Mais aussi :

- ➢ Anonymat strict_____suppression (irréversible) des identités (directes ou indirectes)
- ➢ Pseudo-anonymat_____remplacement (inversible) des identités par des numéros (muets)
- ➢ Vrai-faux anonymat_____modification provisoire (réversible) des informations "ré-identifiantes"

 gilles.trouessin@orange.fr +33 (0)6.63.10.50.76

Qu'est-ce que la *Confidentialité-Discrétion© ?*

Sûreté / sécurité / confidentialité / discrétion / …

La *"confidentialité-discrétion©"* est cette *"propriété qui garantit que les informations sont divulguées en toute discrétion"* :

- Cryptographie_____techniques consistant à protéger l'information électroniquement
- Chiffrement à Clés…_____*exemples :* chiffrement symétrique et chiffrement asymétrique
- Techniques éprouvées_____techniques actuelles pouvant être testées mondialement
- Techniques réversibles_____*exemples :* protection des données durant leur transport

Et aussi :

- En respectant la loi_____longtemps restreinte au *militaire*, la cryptographie s'est assouplie
- Avec l'accord de l'individu_____prendre en compte les exigences émises par la CNIL
- Dans le respect de l'état de l'art_____ces techniques pointues ne s'improvisent pas

© – Gilles Trouessin – 2000-2020 gilles.trouessin@orange.fr +33 (0)6.63.10.50.76

Qu'est-ce que la *Confidentialité-Séclusion©*

Sûreté / sécurité / confidentialité / discrétion / séclusion

La *"confidentialité-séclusion©"* est la *"volonté intime♠♥♦♣ de garantir que les informations sont divulguées entièrement anonymisées"*

- Irréversible_____aucun retour possible depuis les anonymats vers les noms et/ou identités
- Inversible_____seul retour possible aux noms et/ou identités : la voie légale et réglementaire
- Chaînable____possibilité de relier ensemble tous les épisodes de soins et/ou de remboursement
- Robuste_____robustesse aux attaques par inférence (déductives, inductives, abductives, adductives, …)

Et aussi :

- Anonymisation vraie___irréversibilité totale et prouvée (juridique, organisationnelle, technologique)
- Fonction à sens unique_____fonction cryptographique proche du chiffrement irréversible
- Dimension juridique/éthique___organisation indispensable pour garantir un anonymat vrai

♠ [Larousse] « adaptation physiologique par laquelle un animal, une plante ,s'isole du milieu, empêchant passivement les actions défavorables de s'exercer sur lui »
♥ (prononciation & éthymologie) [seklyzjɔ̃] Dérivé savant du latin *seclusum*, supin de *secludere*, signifie: « enfermer à part », « isoler, séparer »
♦ (histoire) 1929 « isolement protecteur d'un organisme par rapport au milieu (ndlr, hostile) » *[ROUSSY, dans Nouv. Traité Médi.fasc. 5. 2. p.76]*
♣ (physiologie) « fait de s'isoler, pour un animal ou une plante, des agressions dues à un milieu défavorable » *[Dictionnaire Français]*

© – Gilles Trouessin – 2000-2020 gilles.trouessin@orange.fr +33 (0)6.63.10.50.76

Qu'est-ce que la sécurité (solutions pour les S.I.S/S.I.H.) ?

La sécurité = assemblage de solutions multiples :

- Politique d'authentification _____ *qui est bien qui il prétend être ?*
- Garantie d'authenticité _____ *qui/comment se porter garant de… ?*
- Contrôle d'accès physique _____ *qui accède à quoi (physiquement) ?*
- Contrôle d'accès logique _____ *qui accède à quoi (informatiquement) ?*
- Gestion des communications _____ *qui échange quoi ? comment ?*
- Modèle d'autorisation _____ *qui décide de "qui a droit à quoi" ?*
- Politique d'autorisation _____ *quoi a le droit d'accéder à quoi ?*
- Politique de lutte anti-infections _____ *lutter contre les virus/ver/spam ?*
- Politique de gestion du personnel _____ *qui affecter sur quelle tâche ?*
- Politique de mise en conformité _____ *qui s'occupe des lois/règlements ?*
- Politique de sensibilisation _____ *qui écrit et promulgue quoi/pourquoi ?*
- Politique d'anonymisation _____ *comment anonymiser/pseudonymiser ?*

 gilles.trouessin@orange.fr +33 (0)6.63.10.50.76

Qu'est-ce que la sécurité (projets pour les S.I.S/S.I.H.) ?

La sécurité = une suite de projets-sécurité à marier :

- Schéma Directeur Sécurité ___ *ou aussi Doctrine Sécurité, Charte Sécurité*
- Schéma Directeur du S.I. _____ *…avec un chapitre « Sécurité du S.I. » ?*
- Charte Informatique _____ *… dont une Charte de l'utilisateur du S.I.*
- Politique d'authentification faible _____ *…utilisation du « Mot De Passe »*
- Politique d'authentification forte _____ *…utilisation d'une carte (CPS)*
- Politique d'autorisation _____ *…avec une matrice des droits d'accès*
- Modèle d'autorisation _____ *…avec gestion des rôles/profils/délégations*
- Gestion des échanges _____ *…distinction entre internes/externes*
- Politique de mise en conformité _____ *…avec des procédures CNIL*
- Politique de sensibilisation _____ *…avec plans de formation/information*
- Politique d'anonymisation _____ *pourquoi / quand / comment anonymiser*
- …

 gilles.trouessin@orange.fr +33 (0)6.63.10.50.76

Qu'est-ce que la sécurité (ISO27002 ou ex-17799 et ISO27799) ?

La sécurité = recueil des meilleures pratiques et/ou Système de Management de la Sécurité des Informations (SMSI) :

- Chap.1- Domaine d'application _____ *Partie 1 (réf. GMSIH)*
- Chap.2- Terminologie et définitions _____ *Partie 1 (réf. GMSIH)*
- Chap.3- Politique de sécurité _____ *Chap.1.1- (réf. GMSIH)*
- Chap.4- Organisation de la sécurité _____ *Chap.1.2- (réf. GMSIH)*
- Chap.5- Classification et contrôles des actifs _____ *Chap.2.1- (réf. GMSIH)*
- Chap.6- Sécurité du personnel _____ *Chap.2.2- (réf. GMSIH)*
- Chap.7- Sécurité physique _____ *Chap.2.3- (réf. GMSIH)*
- Chap.8- Sécurité des communications _____ *Chap.2.4- (réf. GMSIH)*
- Chap.9- Contrôle d'accès (logique) _____ *Chap.2.5- (réf. GMSIH)*
- Chap.10-Développement et maintenance _____ *Chap.2.6- (réf. GMSIH)*
- Chap.11-Gestion de la continuité de l'activité _____ *Chap.2.7- (réf. GMSIH)*
- Chap.12-Conformité (législation et audit) _____ *Chap.2.8- (réf. GMSIH)*

 gilles.trouessin@orange.fr +33 (0)6.63.10.50.76

Qu'est-ce que la sécurité (ex-

La sécurité = recueil des meilleures pratiques ou Système de Management de la Sécurité des Informations (SMSI)

- Chap.1- Domaine d'application _____ *Partie 1 (réf. GMSIH)*
- Chap.2- Terminologie et définitions _____ *Partie 1 (réf. GMSIH)*
- Chap.3- Politique de sécurité _____ *Chap.1.1- (réf. GMSIH)*
- Chap.4- Organisation de la sécurité _____ *Chap.1.2- (réf. GMSIH)*
- Chap.5- Classification et contrôles des actifs _____ *Chap.2.1- (réf. GMSIH)*
- Chap.6- Sécurité du personnel _____ *Chap.2.2- (réf. GMSIH)*
- Chap.7- Sécurité physique _____ *Chap.2.3- (réf. GMSIH)*
- Chap.8- Sécurité des communications _____ *Chap.2.4- (réf. GMSIH)*
- Chap.9- Contrôle d'accès (logique) _____ *Chap.2.5- (réf. GMSIH)*
- Chap.10-Développement et maintenance _____ *Chap.2.6- (réf. GMSIH)*
- Chap.11-Gestion de la continuité de l'activité _____ *Chap.2.7- (réf. GMSIH)*
- Chap.12-Conformité (législation et audit) _____ *Chap.2.8- (réf. GMSIH)*
- …

 gilles.trouessin@orange.fr +33 (0)6.63.10.50.76

PHASE-1 – PRÉSENTATION

Étape-2 – SOLUTIONS : démarche-projet, autorisation, PSSI, etc.

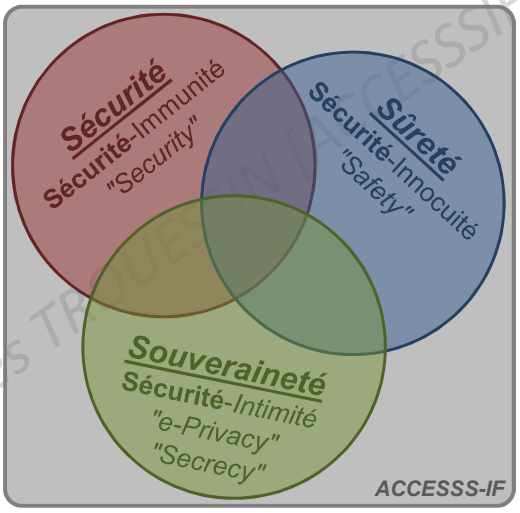
terminologie, définitions, solutions, perspectives, etc.

© – Gilles Trouessin – 2000-2020 gilles.trouessin@orange.fr +33 (0)6.63.10.50.76

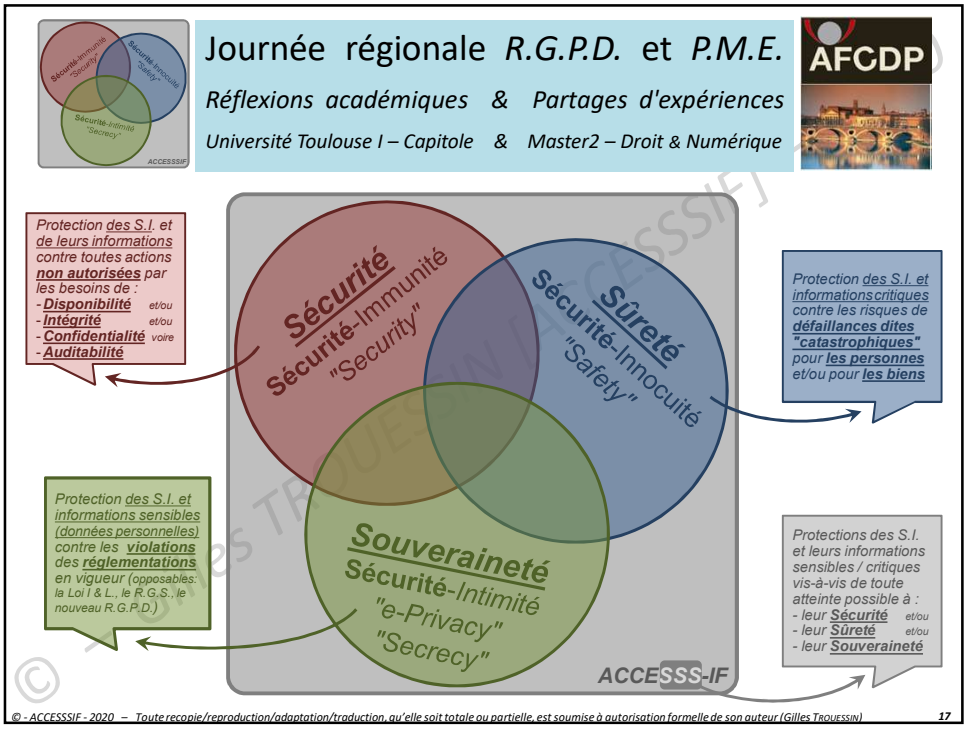
Journée régionale *R.G.P.D.* et *P.M.E.*

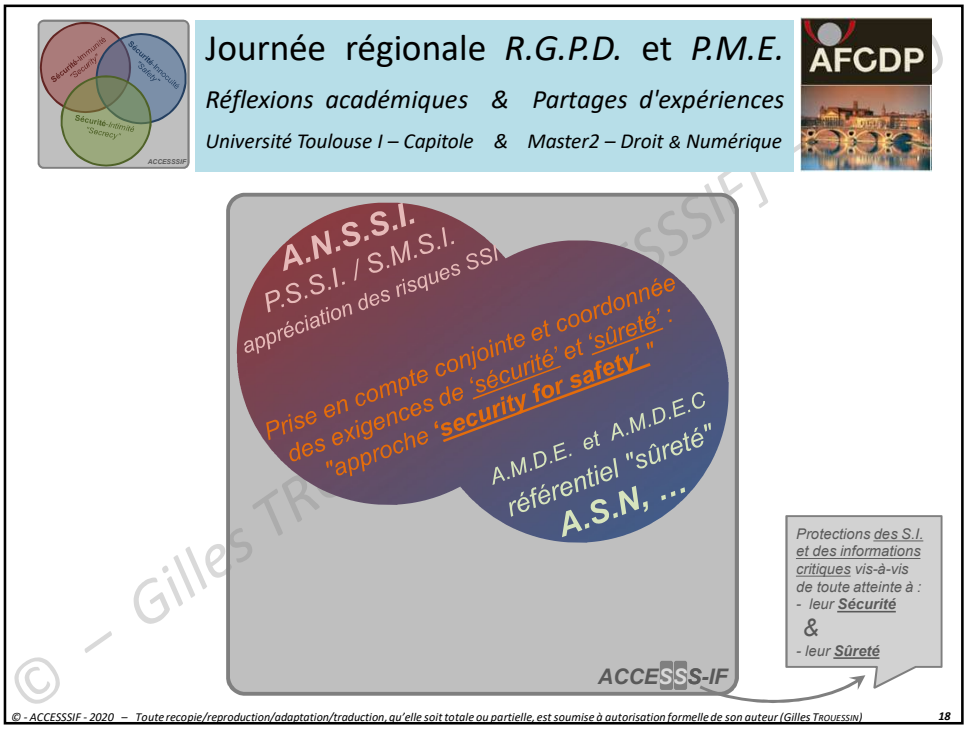
Réflexions académiques & Partages d'expériences

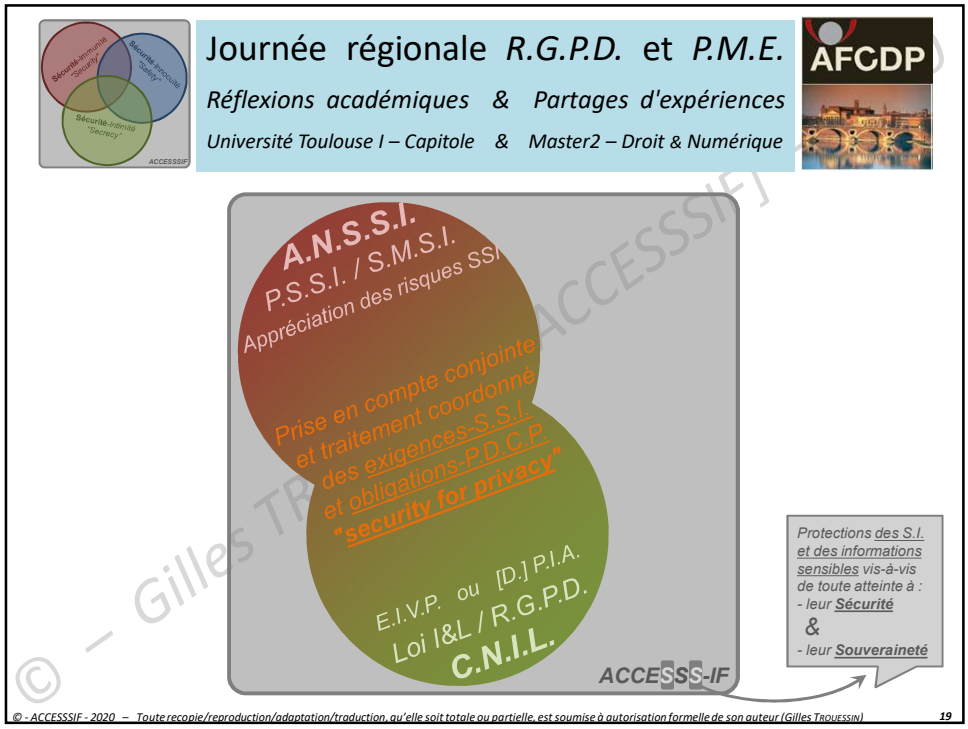
Université Toulouse I – Capitole & Master2 – Droit & Numérique

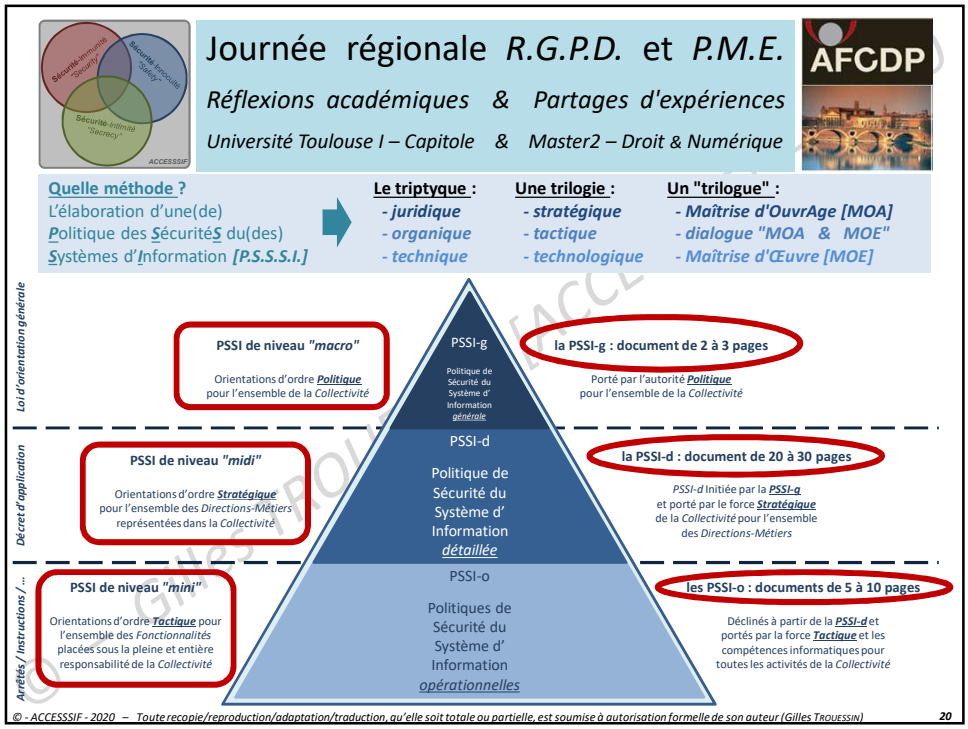


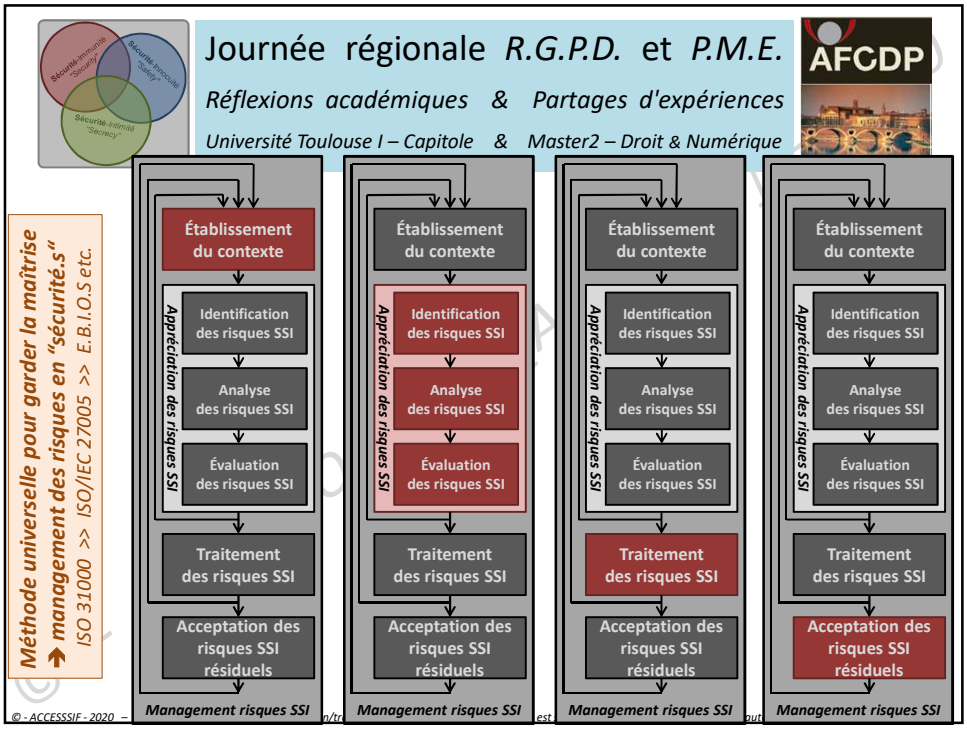
 16

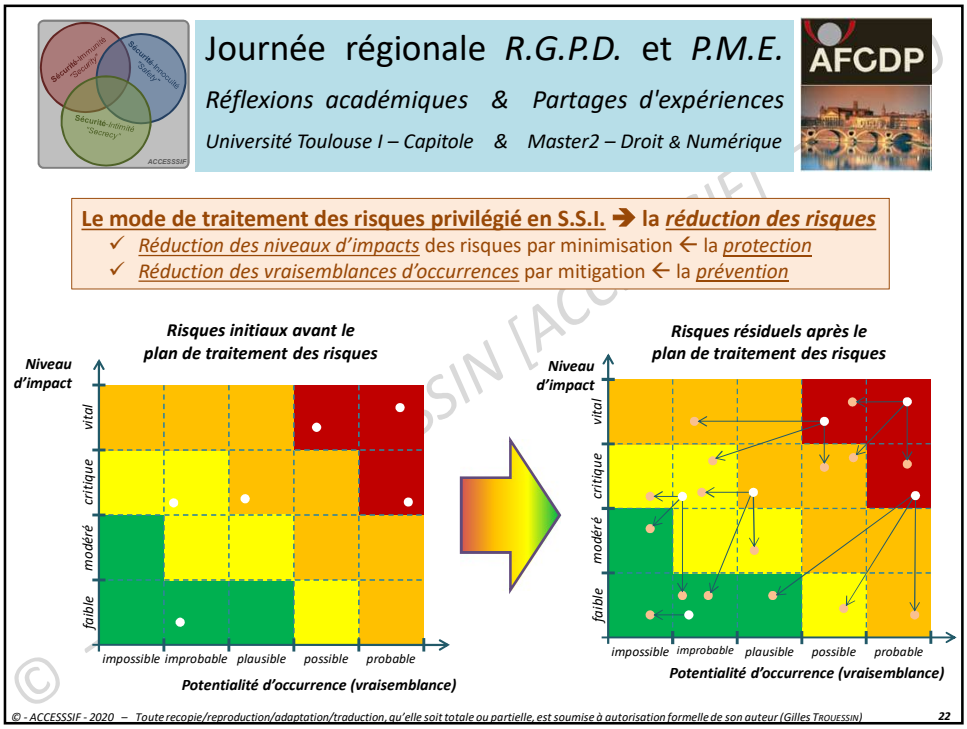

Journée régionale R.G.P.D. et P.M.E.
Réflexions académiques & Partages d'expériences
Université Toulouse I – Capitole & Master2 – Droit & Numérique
AFCDP
Protection des S.I. et de leurs informations contre toutes actions non autorisées par les besoins de :
- Disponibilité et/ou
- Intégrité et/ou
- Confidentialité voire
- Auditabilité
Sécurité
Sécurité-Immunité
"Security"
Sûreté
Sécurité-Innocuité
"Safety"
Souveraineté
Sécurité-Intimité
"e-Privacy"
"Secrecy"
Protection des S.I. et informations critiques contre les risques de défaillances dites "catastrophiques" pour les personnes et/ou pour les biens
Protection des S.I. et informations sensibles (données personnelles) contre les violations des réglementations en vigueur (opposables: la Loi I & L., le R.G.S., le nouveau R.G.P.D.)
Protections des S.I. et leurs informations sensibles / critiques vis-à-vis de toute atteinte possible à :
- leur Sécurité et/ou
- leur Sûreté et/ou
- leur Souveraineté
ACCESSS-IF
© - ACCESSSIF - 2020 – Toute recopie/reproduction/adaptation/traduction, qu'elle soit totale ou partielle, est soumise à autorisation formelle de son auteur (Gilles Trouessin)
17

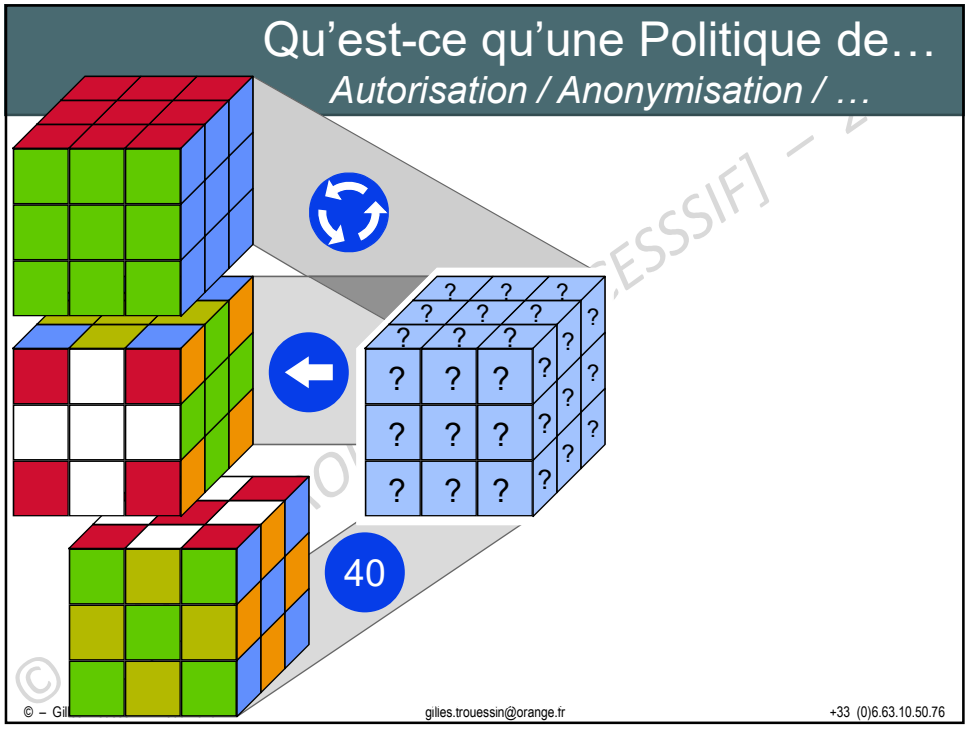

Journée régionale R.G.P.D. et P.M.E.
Réflexions académiques & Partages d'expériences
Université Toulouse I – Capitole & Master2 – Droit & Numérique
AFCDP
A.N.S.S.I.
P.S.S.I. / S.M.S.I.
appréciation des risques SSI
Prise en compte conjointe et coordonnée des exigences de 'sécurité' et 'sûreté' : "approche 'security for safety' "
A.M.D.E. et A.M.D.E.C
référentiel "sûreté"
A.S.N, ...
Protections des S.I. et des informations critiques vis-à-vis de toute atteinte à :
- leur Sécurité
&
- leur Sûreté
ACCESSS-IF
© - ACCESSSIF - 2020 – Toute recopie/reproduction/adaptation/traduction, qu'elle soit totale ou partielle, est soumise à autorisation formelle de son auteur (Gilles Trouessin)
18

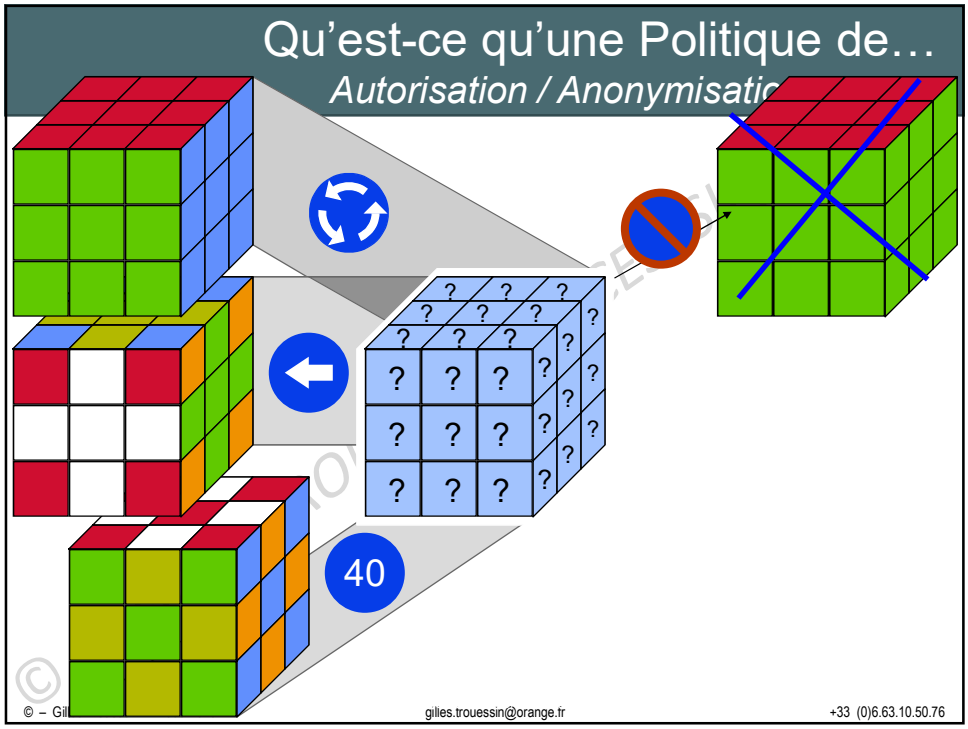

Journée régionale R.G.P.D. et P.M.E.
Réflexions académiques & Partages d'expériences
Université Toulouse I – Capitole & Master2 – Droit & Numérique
AFCDP
A.N.S.S.I.
P.S.S.I. / S.M.S.I.
Appréciation des risques SSI
Prise en compte conjointe et traitement coordonné des exigences-S.S.I. et obligations-P.D.C.P "security for privacy"
E.I.V.P. ou [D.] P.I.A.
Loi I&L / R.G.P.D.
C.N.I.L.
ACCESSS-IF
Protections des S.I. et des informations sensibles vis-à-vis de toute atteinte à :
- leur Sécurité
&
- leur Souveraineté
© - ACCESSSIF - 2020 – Toute recopie/reproduction/adaptation/traduction, qu'elle soit totale ou partielle, est soumise à autorisation formelle de son auteur (Gilles Trouessin)
19

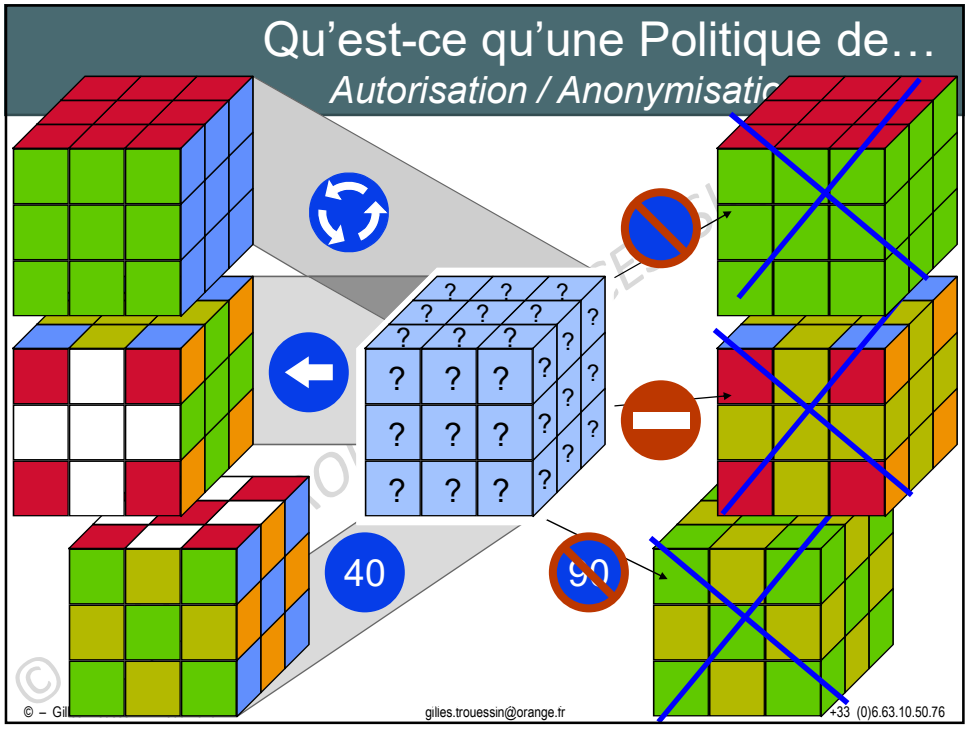

Journée régionale R.G.P.D. et P.M.E.
Réflexions académiques & Partages d'expériences
Université Toulouse I – Capitole & Master2 – Droit & Numérique
AFCDP
Quelle méthode ?
L'élaboration d'une(de)
Politique des Sécurités du(des)
Systèmes d'Information [P.S.S.S.I.]
Le triptyque : - juridique - organique - technique
Une trilogie : - stratégique - tactique - technologique
Un "trilogue" : - Maîtrise d'OuvrAge [MOA] - dialogue "MOA & MOE" - Maîtrise d'Œuvre [MOE]
Loi d'orientation générale
Décret d'application
Arrêtés / Instructions / ...
PSSI de niveau "macro"
Orientations d'ordre Politique pour l'ensemble de la Collectivité
PSSI-g
Politique de Sécurité du Système d' Information générale
la PSSI-g : document de 2 à 3 pages
Porté par l'autorité Politique pour l'ensemble de la Collectivité
PSSI de niveau "midi"
Orientations d'ordre Stratégique pour l'ensemble des Directions-Métiers représentées dans la Collectivité
PSSI-d
Politique de Sécurité du Système d' Information détaillée
la PSSI-d : document de 20 à 30 pages
PSSI-d Initiée par la PSSI-g et porté par le force Stratégique de la Collectivité pour l'ensemble des Directions-Métiers
PSSI de niveau "mini"
Orientations d'ordre Tactique pour l'ensemble des Fonctionnalités placées sous la pleine et entière responsabilité de la Collectivité
PSSI-o
Politiques de Sécurité du Système d' Information opérationnelles
les PSSI-o : documents de 5 à 10 pages
Déclinés à partir de la PSSI-d et portés par la force Tactique et les compétences informatiques pour toutes les activités de la Collectivité
© - ACCESSSIF - 2020 – Toute recopie/reproduction/adaptation/traduction, qu'elle soit totale ou partielle, est soumise à autorisation formelle de son auteur (Gilles Trouessin)
20

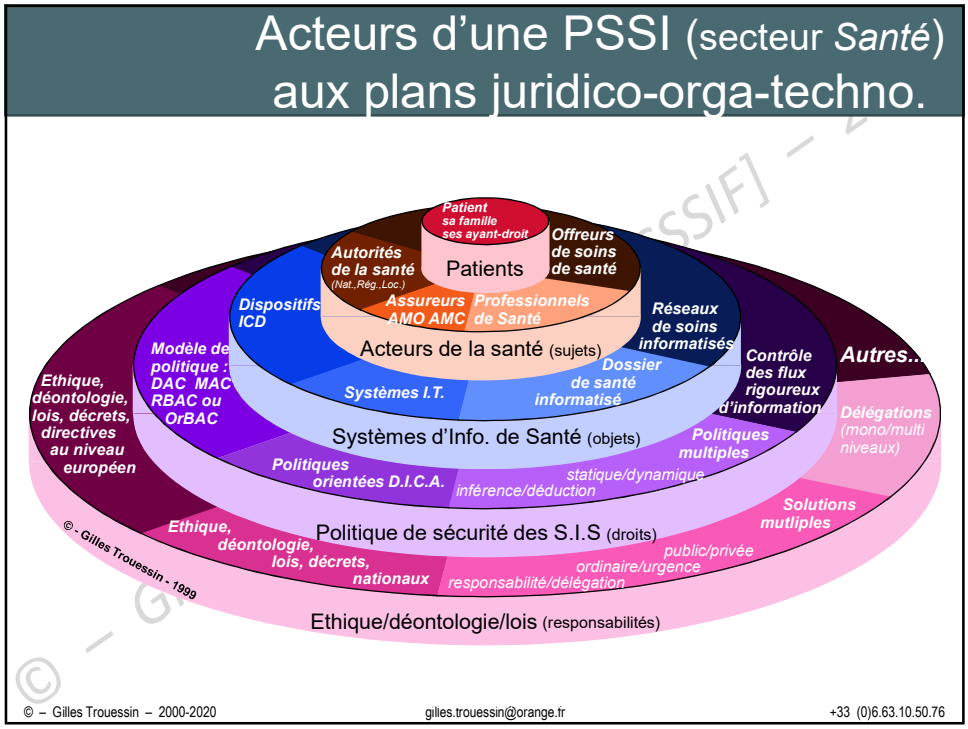

Journée régionale R.G.P.D. et P.M.E.
Réflexions académiques & Partages d'expériences
Université Toulouse I – Capitole & Master2 – Droit & Numérique
AFCDP
Méthode universelle pour garder la maîtrise ➔ management des risques en "sécurité.s" ISO 31000 >> ISO/IEC 27005 >> E.B.I.O.S etc.
Établissement du contexte
Appréciation des risques SSI
Identification des risques SSI
Analyse des risques SSI
Évaluation des risques SSI
Traitement des risques SSI
Acceptation des risques SSI résiduels
Management risques SSI


Journée régionale R.G.P.D. et P.M.E.
Réflexions académiques & Partages d'expériences
Université Toulouse I – Capitole & Master2 – Droit & Numérique
AFCDP
Le mode de traitement des risques privilégié en S.S.I. ➔ la réduction des risques
✓ Réduction des niveaux d'impacts des risques par minimisation ← la protection
✓ Réduction des vraisemblances d'occurrences par mitigation ← la prévention
Risques initiaux avant le plan de traitement des risques
Risques résiduels après le plan de traitement des risques
Niveau d'impact
vital
critique
modéré
faible
impossible improbable plausible possible probable
Potentialité d'occurrence (vraisemblance)
© - ACCESSSIF - 2020 – Toute recopie/reproduction/adaptation/traduction, qu'elle soit totale ou partielle, est soumise à autorisation formelle de son auteur (Gilles Trouessin)
22


Qu’est-ce qu’une Politique de…
Autorisation / Anonymisation / …
40
© – Gil
gilles.trouessin@orange.fr
+33 (0)6.63.10.50.76


Qu’est-ce qu’une Politique de…
Autorisation / Anonymisatio
40
© – Gil
gilles.trouessin@orange.fr
+33 (0)6.63.10.50.76


Qu'est-ce qu'une Politique de…
Autorisation / Anonymisatio
40
90
© – Gil
gilles.trouessin@orange.fr
+33 (0)6.63.10.50.76


Acteurs d'une PSSI (secteur Santé)
aux plans juridico-orga-techno.
Patient
sa famille
ses ayant-droit
Patients
Autorités
de la santé
(Nat.,Rég.,Loc.)
Offreurs
de soins
de santé
Dispositifs
ICD
Assureurs
AMO AMC
Professionnels
de Santé
Réseaux
de soins
informatisés
Acteurs de la santé (sujets)
Modèle de
politique :
DAC MAC
RBAC ou
OrBAC
Systèmes I.T.
Dossier
de santé
informatisé
Contrôle
des flux
rigoureux
d'information
Autres...
Ethique,
déontologie,
lois, décrets,
directives
au niveau
européen
Systèmes d'Info. de Santé (objets)
Politiques
multiples
Délégations
(mono/multi
niveaux)
Politiques
orientées D.I.C.A.
statique/dynamique
inférence/déduction
Solutions
mutliples
Ethique,
déontologie,
lois, décrets,
nationaux
Politique de sécurité des S.I.S (droits)
public/privée
ordinaire/urgence
responsabilité/délégation
© - Gilles Trouessin - 1999
Ethique/déontologie/lois (responsabilités)
© – Gilles Trouessin – 2000-2020
gilles.trouessin@orange.fr
+33 (0)6.63.10.50.76

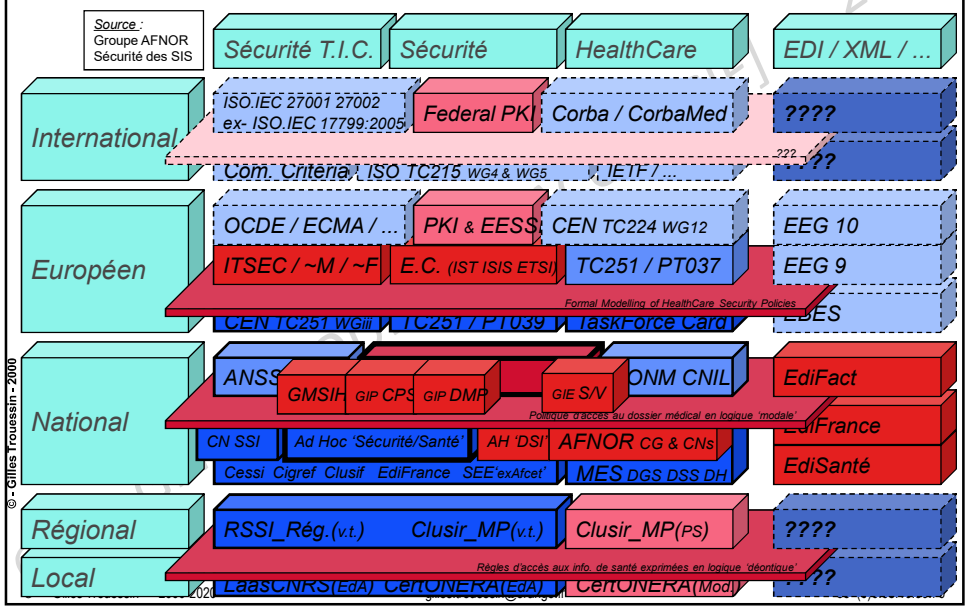
PHASE-1 – PRÉSENTATION

Étape-3 – SOLUTIONS : retours d'expériences, savoir-faire, etc.

terminologie, définitions, solutions, perspectives, etc.

© – Gilles Trouessin – 2000-2020 gilles.trouessin@orange.fr +33 (0)6.63.10.50.76

Normes *'de jure'* & Standards



Enseignements autour de la sécurité du DMP ?

DISPONIBILITE

- Besoins :
  - Accessibilité ?
  - Disponibilité ?
  - Réactivité ?
- Objectifs :
  - Services au patient ?
  - Consentement expresse ?
- Exigences :
  - Redondance totale ?
  - Archivages en ligne ?
  - Backup en temps réel ?
  - Stockage centralisé ?
  - Stockage distribué ?
  - Stockage réparti ?

INTEGRITE

- Besoins :
  - Intégrité ?
  - Intégralité ?
  - Exhaustivité ?
- Objectifs :
  - Services aux PS ?
  - Mandats implicites ?
- Exigences :
  - Mémoire intégrale ?
  - Conservation partielle ?
  - *"Gestion"* par le patient ?
  - Checksum *'numérique'* ?
  - Signature *'électronique'* ?
  - Opposabilité et preuves

CONFIDENTIALITE

- Besoins :
  - Confidentialité ?
  - Discrétion ?
  - Anonymat ?
- Objectifs :
  - Réversibilité ?
  - Inversibilité ?
  - Irréversibilité ?
- Exigences :
  - Chaînage des "noms" et/ou des identités/identifiants ?
  - Algorithmes de chiffrement : robustesse aux attaques ?
  - Clés cryptographiques : choix des crypto-périodes ?
  - TPC(TTP) / IGC(PKI) et autres lieux de confiance ?

Disponibilité, intégrité, confidentialité(s) : le risque-DMP / les risques pour un DMP

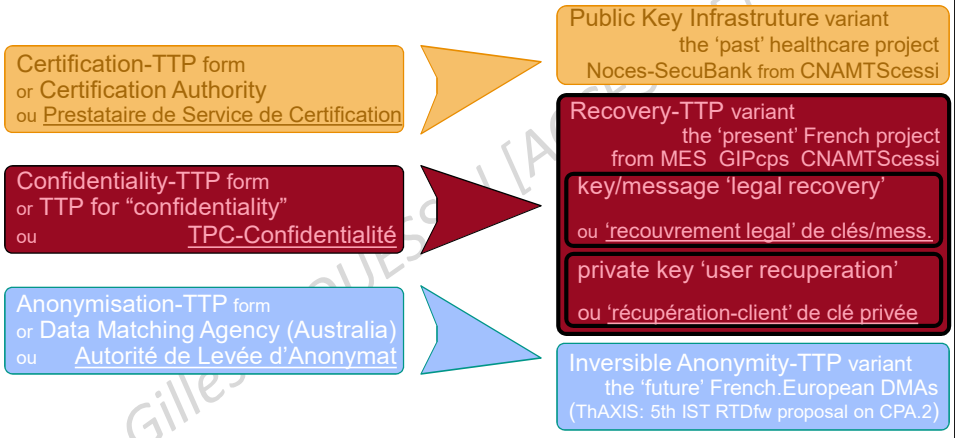
- **Disponibilité : obligation** d'accessibilité, de réactivité et de connectivité
- **Intégrité : obligation** de complétude, correction, précision et d'exactitude
- **Confidentialité-discrétion© : obligation** de protection et de discrétion
  - Les risques résident dans une **mauvaise application** des **techniques de base**
  - Les parades consistent à faire, ou faire faire, une veille cryptographique constante et à intégrer les outils de chiffrement/signature dans la chaîne logique de la sécurité
  - Les solutions passent par l'**analyse** de risques et l'**expression** des besoins
- **Confidentialité-séclusion© : interdic.** atteinte à l'intimité et à la vie privée
  - Les risques sont plus **difficilement mesurables** car les impacts souvent **irréparables**
  - Les menaces sont de trois ordres : **juridiques**, organisationnels et technologiques
  - Les conséquences peuvent être **définitives** tant pour le **"fautif"** que pour la **"victime"**
  - Les solutions passent par une analyse **fine** des risques, l'expression **précise** des besoins

Intimité/innocuité - consentement/preuve : le risque-DMP / les risques pour un DMP

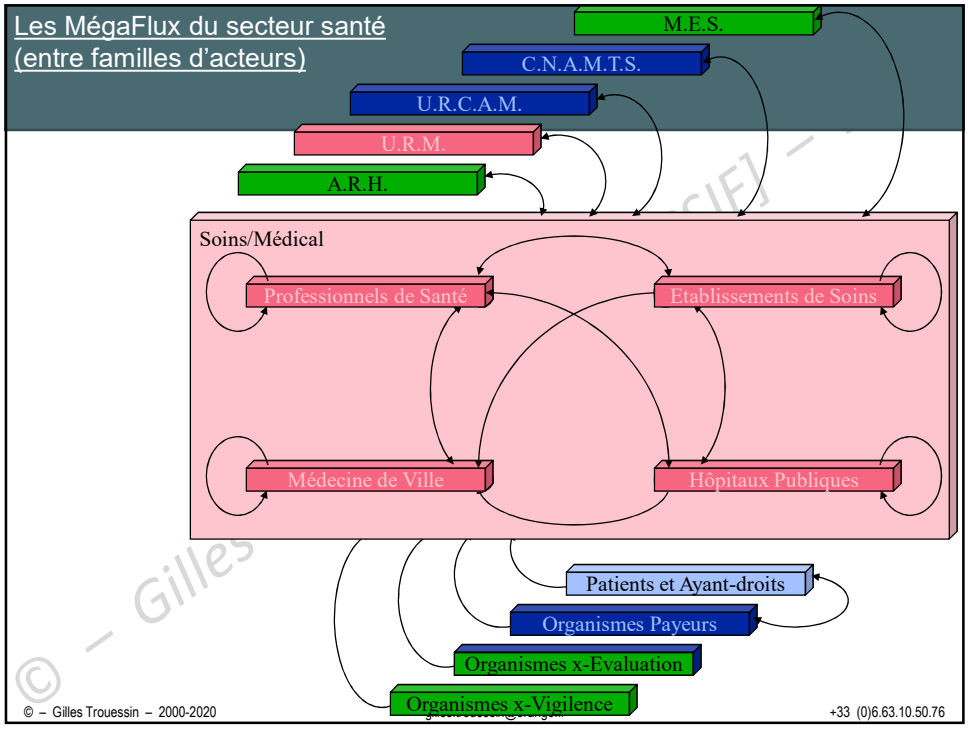
- **Intégralité *versus* Intégrité : obligation** de moyen et/ou de résultat
  - Intégralité (exhaustivité) : l'entièreté de l'information est-elle nécessaire pour contribuer à améliorer la continuité des soins et pour permettre le soin « sans couture » ?
  - Intégrité (exactitude) : la véracité des informations est-elle suffisante pour garantir la cohérence des informations et pour permettre la cohérence des soins ?
- **Traçabilité *versus* Opposabilité : nécessité** de trouver un compromis
  - Traçabilité (imputabilité) : face au compromis entre choix (privatif) et décision (médicale), comment préserver le soigné (respect de son intimité) et ménager le soignant (éléments de preuve) ?
  - Opposabilité (irréfragabilité) : face à la légitimité de lire, écrire ou modifier des données, comment distinguer "habilitation d'accès (générique)" et "autorisation d'accéder (spécifique)" ?
- **Droit à l'oubli *versus* Droit de défense : intérêt(s) individuel / collectif**
  - Droit à l'oubli pour le soigné : avec le droit du patient à (contribuer à) gérer ses données, jusqu'où peut aller le consentement du patient (le « colloque singulier » est-il toujours envisageable ?) ?
  - Droit de défense du soignant : pour une permanence/persistance/pérennité des données, jusqu'où peut aller l'admissibilité en preuve (le « secret médical/prof. » est-il toujours d'ordre public ?) ?

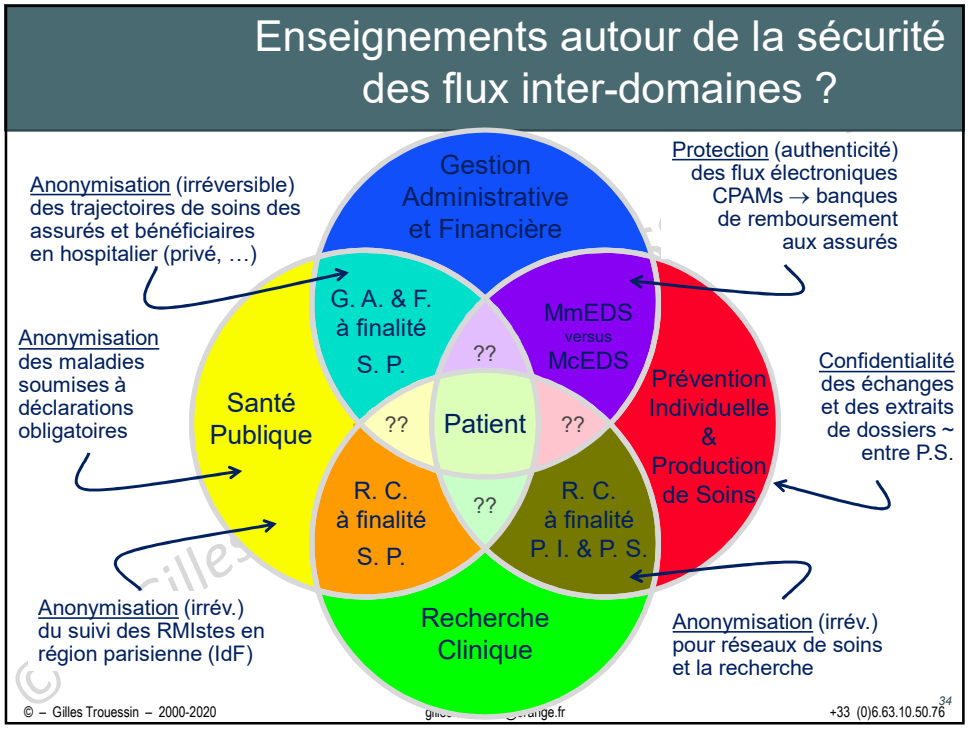
 gilles.trouessin@orange.fr +33 (0)6.63.10.50.76

Enseignements autour de la sécurité du Tierces Parties de Confiance ?

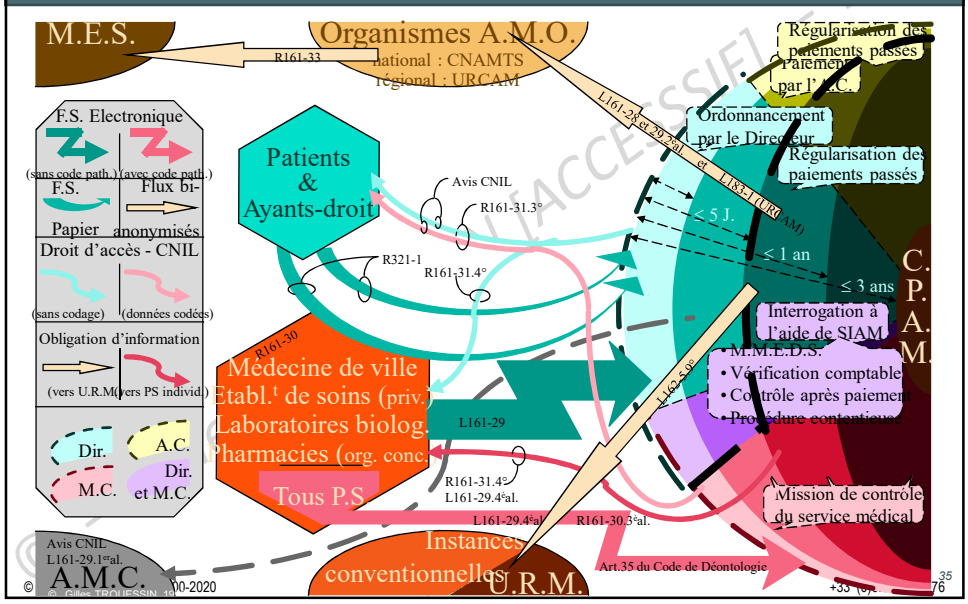


 gilles.trouessin@orange.fr +33 (0)6.63.10.50.76 32

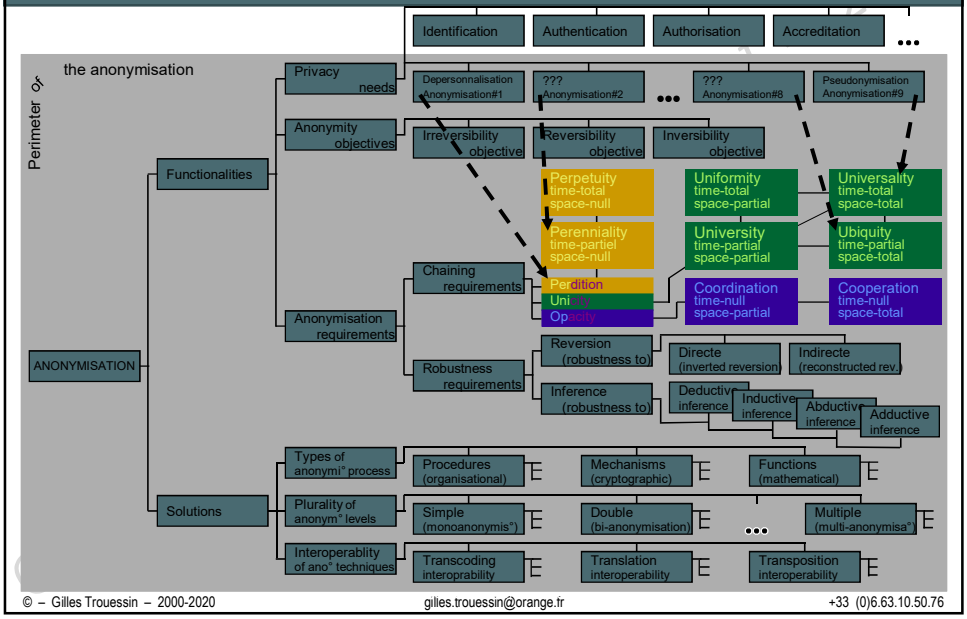

Les MégaFlux du secteur santé
(entre familles d'acteurs)
M.E.S.
C.N.A.M.T.S.
U.R.C.A.M.
U.R.M.
A.R.H.
Soins/Médical
Professionnels de Santé
Etablissements de Soins
Médecine de Ville
Hôpitaux Publiques
Patients et Ayant-droits
Organismes Payeurs
Organismes x-Evaluation
Organismes x-Vigilence
© – Gilles Trouessin – 2000-2020
+33 (0)6.63.10.50.76


Enseignements autour de la sécurité des flux inter-domaines ?
Anonymisation (irréversible) des trajectoires de soins des assurés et bénéficiaires en hospitalier (privé, …)
Protection (authenticité) des flux électroniques CPAMs → banques de remboursement aux assurés
Anonymisation des maladies soumises à déclarations obligatoires
Confidentialité des échanges et des extraits de dossiers ~ entre P.S.
Anonymisation (irrév.) du suivi des RMIstes en région parisienne (IdF)
Anonymisation (irrév.) pour réseaux de soins et la recherche
Gestion Administrative et Financière
G. A. & F. à finalité S. P.
MmEDS versus McEDS
Santé Publique
Prévention Individuelle & Production de Soins
Patient
??
R. C. à finalité S. P.
R. C. à finalité P. I. & P. S.
Recherche Clinique
© – Gilles Trouessin – 2000-2020
+33 (0)6.63.10.50.76
34

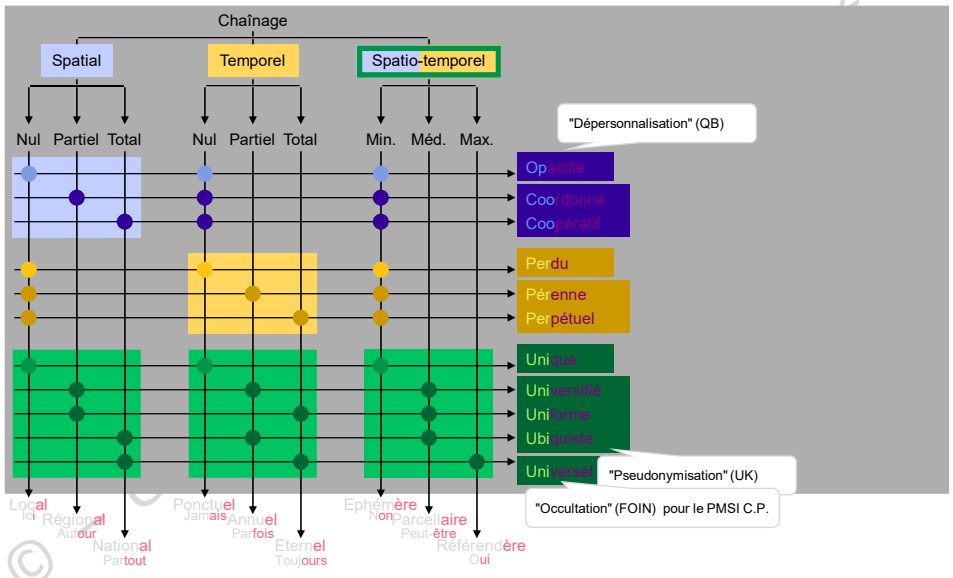
Enseignements autour de la sécurité des flux de/vers l'AMO ?



"Taxonomie" en « anonymisation » (suppression des éléments nominatifs)

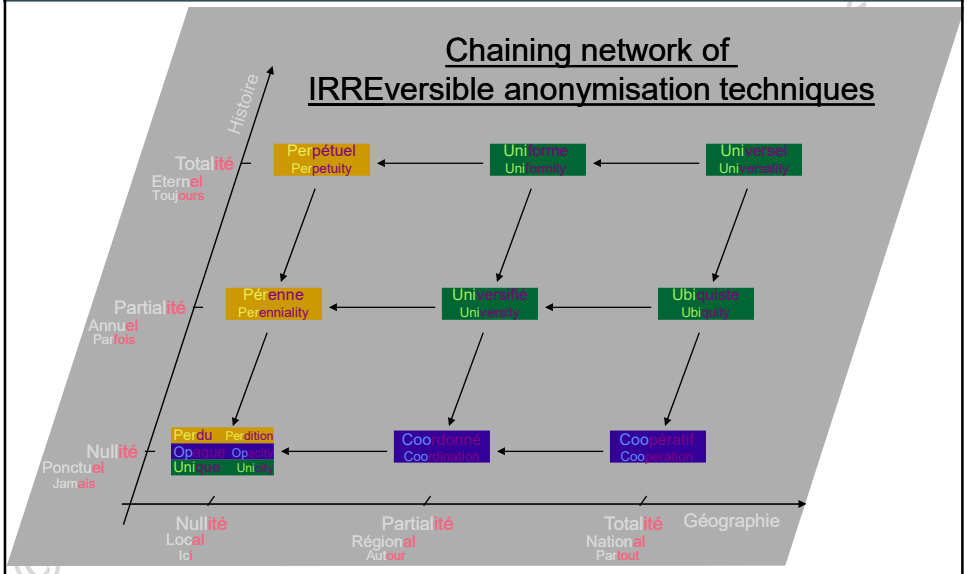


"Variantes" en « pseudonymisation »
(anonymisation avec chaînage)



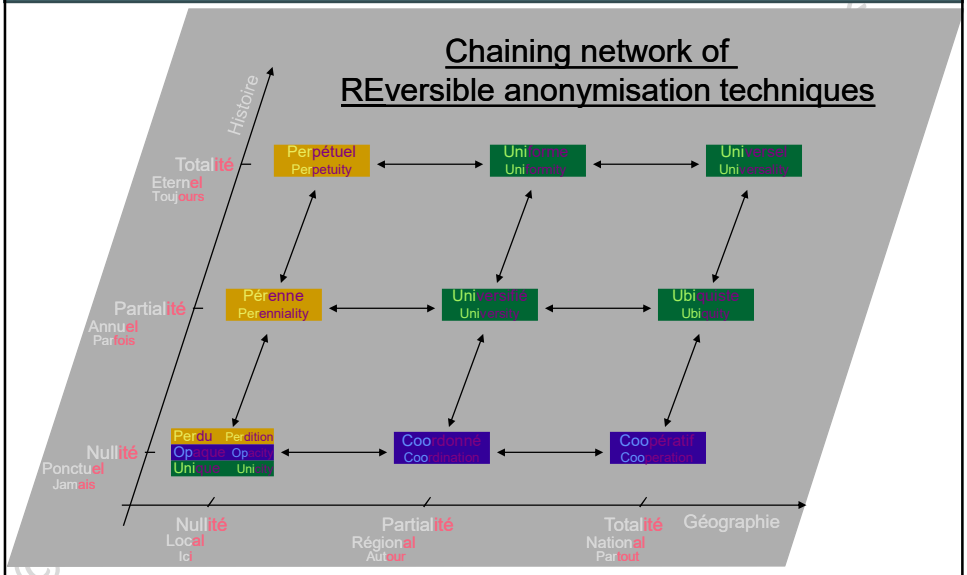
 gilles.trouessin@orange.fr +33 (0)6.63.10.50.76

"Hiérarchie" en « hétéronymisation »
(pseudonymisation avec diversification)



 gilles.trouessin@orange.fr +33 (0)6.63.10.50.76

"Hiérarchie" en « hétéronymisation »
(pseudonymisation avec diversification)



 gilles.trouessin@orange.fr +33 (0)6.63.10.50.76

PHASE-2 – DISCUSSIONS-DÉBAT

avis/suggestions/remarques, questions/réponses, besoins, etc.

[pour prolonger cette présentation]

❖

Je vous remercie
pour votre attention.

❖

 gilles.trouessin@orange.fr +33 (0)6.63.10.50.76