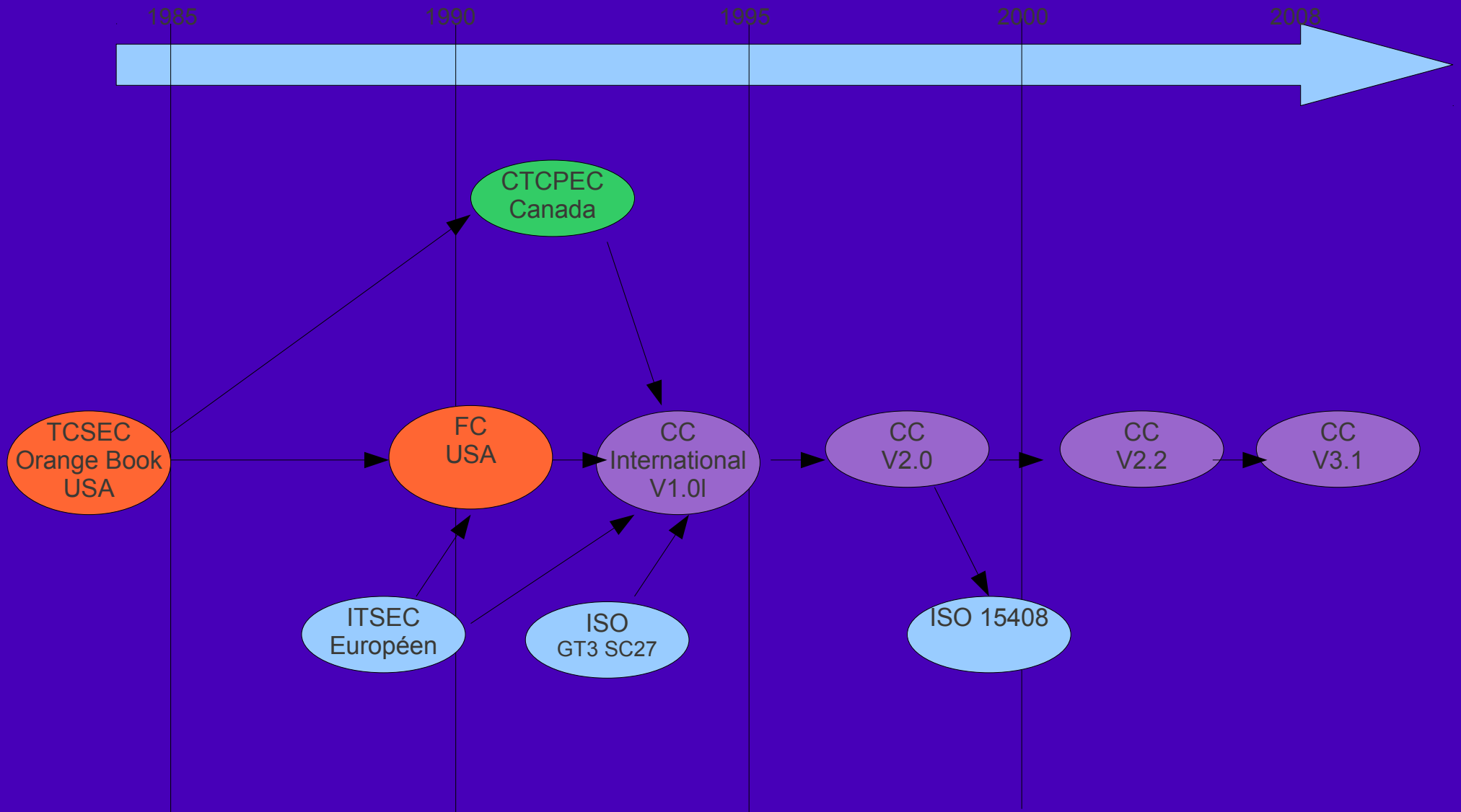


Qualification produit (RGS) & Logiciel Libre

www.clusir-aquitaine.fr

Historique



Critères Communs

Objectifs :

S'assurer qu'un produit couvre les risques de façon :

Cohérente

Complète

Résistante

Une reconnaissance réciproque fondée sur un schéma d'évaluation reconnu



CC : Principes

Une démarche :

Une démarche préalable d'analyse de risques

Des fonctions de sécurité qui répondent à des risques identifiés

Une vérification de couverture dans le cadre d'un document de spécifications (cible de sécurité)

Un catalogue structuré de fonctions de sécurité

Des classes d'assurance

Une méthode pour le développement et/ou le contrôle des produits de sécurité

CC : un cahier des charges fonctionnel

Présentation de la cible d'évaluation (TOE)

Définition des contexte de sécurité

Biens, Menaces, Politique de sécurité organisationnelle, hypothèses

Objectifs de sécurité

Pour la « TOE », pour l'environnement

Argumentaire (Justification de la couverture)

Exigences de sécurité

Fonctions de sécurité (exigences)

Exigences d'assurance

Argumentaire (Justification de la complétude, de la cohérence et de la résistance)

CC : Des classes assurantielles

Classe d'assurance	Famille d'assurance	Abréviation
Classe ACM : Gestion de configuration	Automatisation de la CM	ACM_AUT
	Capacités de la CM	ACM_CAP
	Portée de la CM	ACM_SCP
Classe ADO : Livraison et exploitation	Livraison	ADO_DEL
	Installation, génération et démarrage	ADO_IGS
Classe ADV : Développement	Spécifications fonctionnelles	ADV_FSP
	Conception de haut niveau	ADV_HLD
	Représentation de l'implémentation	ADV_IMP
	Parties internes de la TSF	ADV_INT
	Conception de bas niveau	ADV_LLD
	Correspondance des représentations	ADV_RCR
	Modélisation de la politique de sécurité	ADV_SPM
Classe AGD : Guides	Guide de l'administrateur	AGD_ADM
	Guide de l'utilisateur	AGD_USR
Classe ALC : Support au cycle de vie	Sécurité du développement	ALC_DVS
	Correction d'anomalies	ALC_FLR
	Définition du cycle de vie	ALC_LCD
	Outils et techniques	ALC_TAT
Classe ATE : Tests	Couverture	ATE_COV
	Profondeur	ATE_DPT
	Tests fonctionnels	ATE_FUN
	Tests indépendants	ATE_IND
Classe AVA : Estimation des vulnérabilités	Analyse des canaux cachés	AVA_CCA
	Utilisation impropre	AVA_MSU
	Résistance des fonctions de sécurité de la TOE	AVA_SOF
	Analyse de vulnérabilités	AVA_VLA

CC 7 niveaux d'assurance

EAL1 : testé fonctionnellement

EAL2 : testé structurellement

EAL3 : testé et vérifié méthodiquement

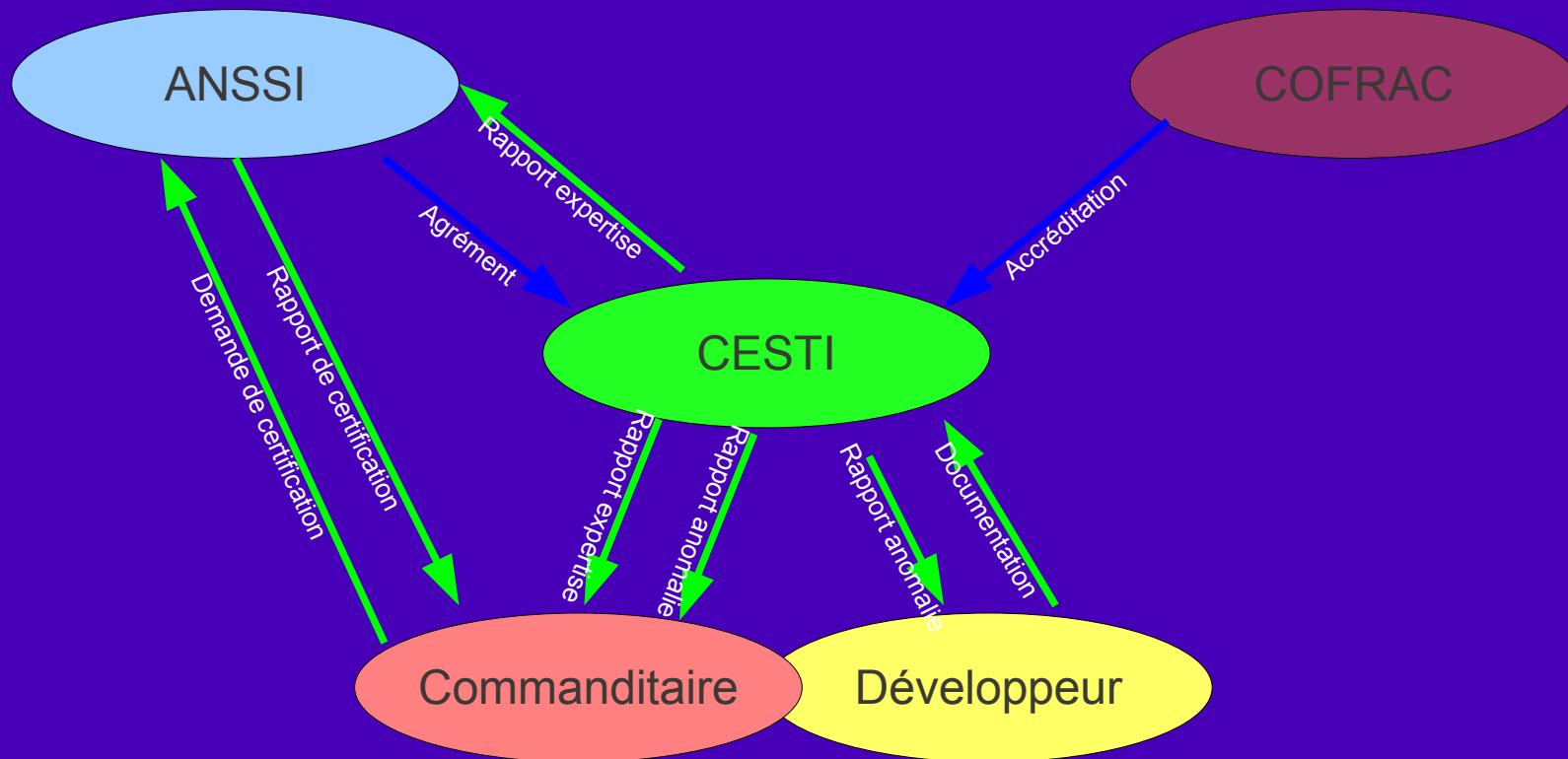
EAL4 : conçu, testé et vérifié méthodiquement,

EAL5 : conçu de façon semi-formelle et testé

EAL6 : conception vérifiée de façon semi-formelle et testé

EAL7 : conception vérifiée de façon formelle et testée.

Le schéma national d'évaluation



Les CESTI Logiciel

OPPIDA
SILICOMP-AQL
AMOSYS (en cours)
8/2828

Contexte Français : RGS

Issue de l'ordonnance de 2005 visant à mettre en place les principes de la confiance pour l'e-administration

Accessibilité ;

Interopérabilité ;

Sécurité

Fondé sur 3 grands dispositifs :

Gestion des risques et homologation

Qualification des produits de sécurité

Référentiel intersectoriel pour les politiques de certification (Authentification, signature, confidentialité, horodatage)

RGS - Qualification des produits

3 niveaux d'assurances

Élémentaire (CSPN)

Standard (CC)

Renforcé (CC)

Un principe commun :

Une cible de sécurité décrivant les risques couverts et validée par l'ANSSI

Standard et renforcé fondés sur les CC:

Standard : EAL3 +

Renforcé : EAL4 +

RGS : Qualification

Le choix des qualifications en fonction du niveau des usages PRIS :

Authentification

Confidentialité

Signature

Authentification Serveur

Cachet

Standard / Renforcé

Standard

Renforcé

Assurance class	Assurance Family	Assurance Components by						
		Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Configuration management	ACM AUT				1	1	2	2
	ACM CAP	1	2	3	4	4	5	5
	ACM SCP			1	2	3	3	3
Delivery and operation	ADO DEL		1	1	2	2	2	3
	ADO IGS	1	1	1	1	1	1	1
Development	ADV FSP	1	1	1	2	3	3	4
	ADV HLD		1	2	2	3	4	5
	ADV IMP				1	2	3	3
	ADV INT					1	2	3
	ADV LLD				1	1	2	2
	ADV RCR	1	1	1	1	2	2	3
	ADV SPM				1	3	3	3
Guidance documents	AGD ADM	1	1	1	1	1	1	1
	AGD USR	1	1	1	1	1	1	1
Life cycle support	ALC DVS			1	1	1	2	2
	ALC FLR							
	ALC LCD				1	2	2	3
	ALC TAT				1	2	3	3
Tests	ATE COV		1	2	2	2	3	3
	ATE DPT			1	1	2	2	3
	ATE FUN		1	1	1	1	2	2
	ATE IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA CCA					1	2	2
	AVA MSU			1	2	2	3	3
	AVA SOF		1	1	1	1	1	1
	AVA VLA		1	1		3	4	4

CSPN

Une cible de sécurité simplifiée

Une évaluation en temps contraint (25j/h)

Des centres d'évaluation plus nombreux

Une analyse de conformité et d'efficacité sur le produit fini

Pas d'évaluation en terme de processus de développement

CSPN : produits

Produits	Domaine	Commanditaire
Dispositif d'échange sécurisé d'informations sans interconnexion réseau (DESIIR) v1.0	Parefeux	EDF R&D
Logiciel UCOPIA pour boîtiers appliances UCOPIA version 3.0 release 5	Parefeux	UCOPIA Communications
Bro v1.4	Détection d'intrus	Berkeley USA / ANSSI
VSC-TOOAL v1.1	Authentification	Mediscs / Mediscs
Netfilter sur un noyau Linux v2.6.27 - iptables v1.4.2	Parefeux	Netfilter Core Team / SGDN

Les éléments de la confiance dans le développement

Le PAQ générique

- assurance qualité et niveau de service ;
- organisation, communication, pilotage ;
- gestion de la qualité du logiciel ;
- méthode de développement logiciel ;
- gestion des exigences ;
- gestion du plan de tests ;
- gestion des divergences ;
- gestion quantitative des charges ;
- gestion de la planification ;
- gestion de la documentation ;
- gestion " pragmatique " des risques ;

Les éléments de la confiance dans le développement

2 AXES

Gestion de projet

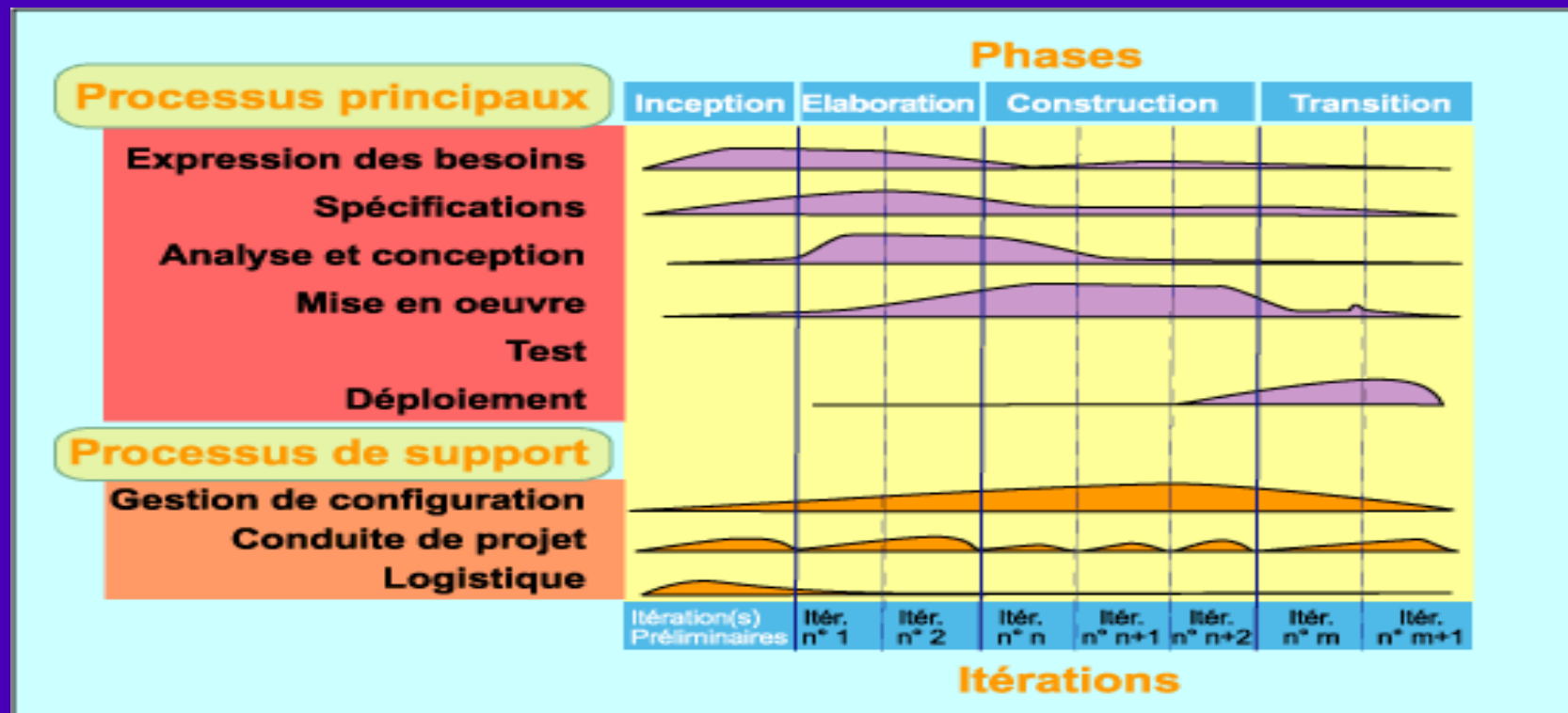
- ✓ Pilotage (prise de décision, PAQ, financier)
- ✓ Planification
- ✓ Gestion de configuration

Processus de développement (Itératif, incrémental)

- ✓ Analyse
- ✓ Conception
- ✓ Développement
- ✓ Test unitaire
- ✓ Recette, livraison, déploiement

Les éléments de la confiance dans le développement

Le cycle de vie d'un projet de développement logiciel



Les éléments de la confiance dans le développement

Les méthodes associées aux processus de développement

Unified process (Basé sur un modèle exécutable)

RUP, 2TUP

Méthode agile (Basé sur des bonnes pratiques)

RAD, XP, DSDM, ASD, FDD, Scrum, Crystal clear

Aspects	Facteurs de succès	Causes d'échecs
Politique	Le directeur du projet et/ou le responsable du groupe d'animation et de rapport répond à une autorité supérieure (à la direction générale dans un projet stratégique)	Le directeur de projet ne dispose pas d'un mandat suffisant pour arbitrer les divers intervenants, limiter leurs luttes d'influence, leurs ambitions ou visions partisans.
Pilotage	Piloter le projet <i>dynamiquement</i> essentiellement par les enjeux et les risques .	Piloter le projet <i>administrativement</i> essentiellement par les budgets et les ressources .
Organisation	Engager un mode projet centralisant sur un plateau unique tous les intervenants aussi bien sur le plan organisationnel que géographique. Formaliser dans le cadre de courtes missions de réelles délégations de responsabilité verticales et latérales.	Utiliser des ressources à temps partiel et/ou non dépendantes directement de la direction de projet. Ne pas disposer de l'agenda électronique de l'ensemble des intervenants. Négliger la couverture des participants en terme de responsabilité hiérarchique.
Financier	Justifier le projet par un plan d'investissement global mais simple , dont chaque élément est une base réaliste et acceptée.	Créer et maintenir un modèle financier dont le niveau de détail interdit ensuite sa remise en question et dont la complexité fera ensuite douter de sa pertinence .
Planification	Intégrer dès le début du projet l'ensemble des sous-projets et des contraintes dans un planning réaliste qui sera ensuite suivi jalon par jalon avec un outil professionnel léger.	Négliger un contrôle approfondi sur l'avancement des diverses parties sous traitées ou réalisées dans des sites éloignés de la direction du projet
Innovation	Viser l'utilisation de <i>technologies émergentes</i> dont la stabilisation est prévue pour la date du déploiement afin d'obtenir l'optimum d'efficacité stratégique	Se limiter aux technologies ou puissance de machine <i>disponible à la date du cahier des charges</i> ou de la réalisation pour des raisons administratives ou contractuelles
Communication	Employer un groupe d'animation et de rapport disposant de moyens modernes pour dynamiser la communication ainsi que formaliser et centraliser l'information.	Ne pas distinguer les groupes de travail de ceux de validation . Laisser les intervenants organiser en permanence des réunions <i>brainstorming</i> , non préparées ou non structurées et à participation variable.
Méthode	Cycle de vie itératif incrémentiel : réaliser des livraisons de résultats partiels sous la forme de plusieurs Focus de validation, suivis d'un prototype final, puis d'un site pilote.	Cycle de vie cascade classique : avant même de lever les risques organisationnels ou techniques, viser directement un système totalement finalisé dans la vision d'un déploiement total et parfait.

Principe et Problématiques du développement communautaire

PLAN

Les Acteurs génériques

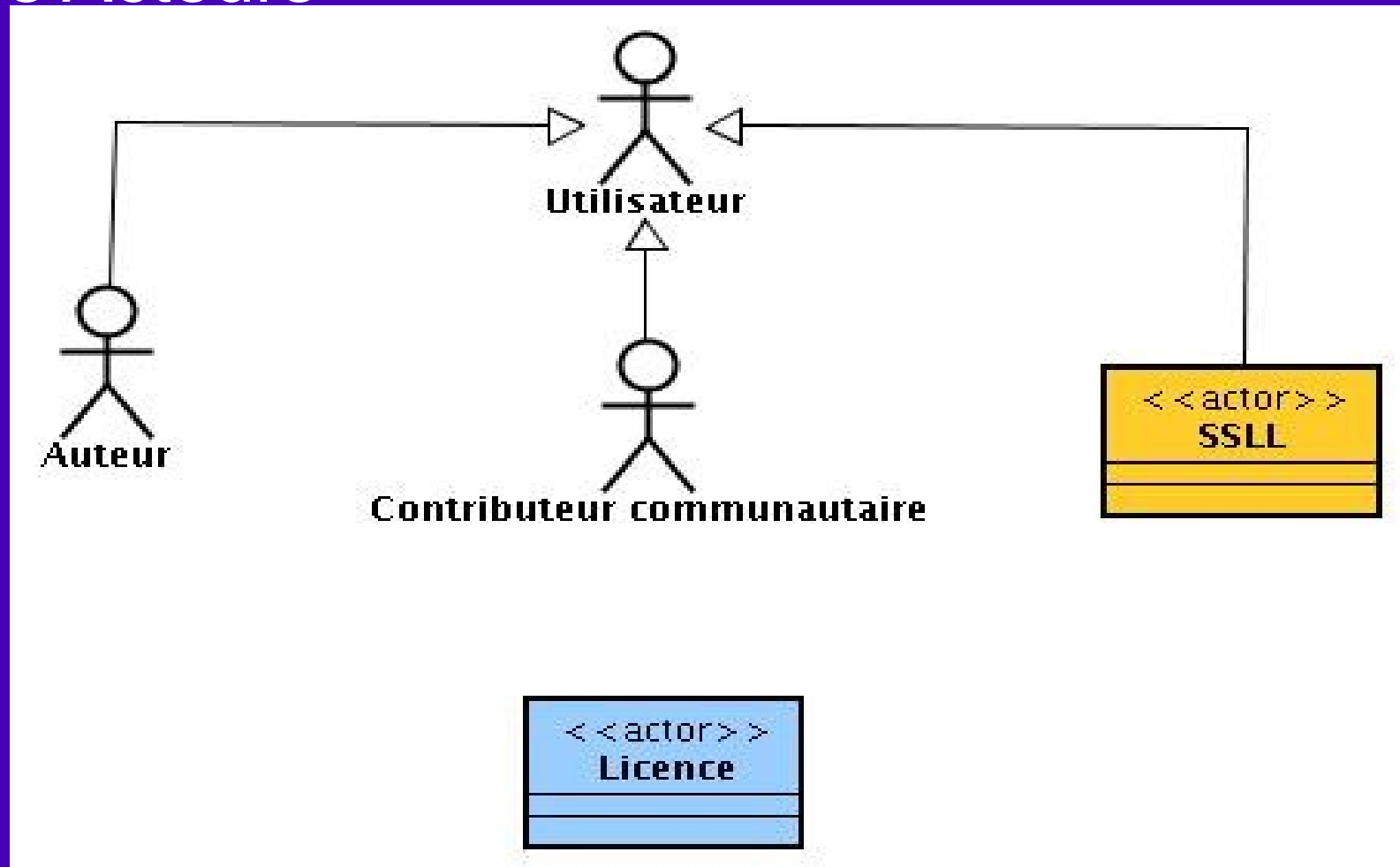
Les 3 phases d'un projet Open Source

Les Risques liés à un projet Open Sources

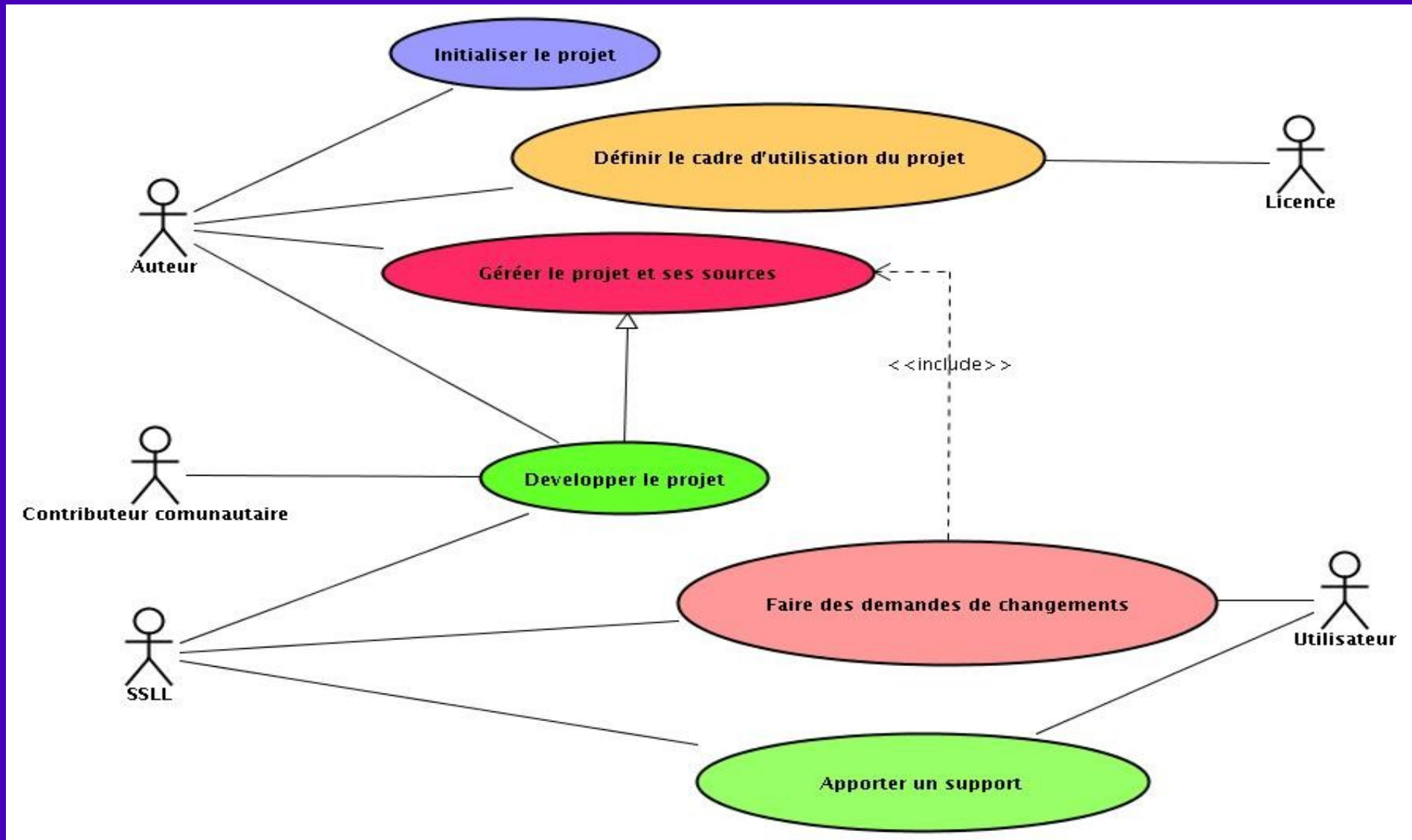
Exemple de projet Open Source ayant obtenu une certification CSPN

Les Acteurs du développement communautaire

Les Acteurs



Les Acteurs du développement communautaire



Les 3 phases d'un projet Open Source

- Développement Initial
 - Mise en place du projet et des outils collaboratifs (FORGES)
- Formation à la communauté
 - appel à contribution
- Business
 - Distribution, contrat de maintenance avec des entreprises, moyennent contre partie financière

Les Risques liés à un projet Open Sources

- Risques liés aux Utilisateurs
 - demandes contraires à l'utilisation
 - copie d'une demande déjà existante
 - manque de retour sur un dysfonctionnement
- Risques liés à la communauté
 - fork
- Risques liés à l'Auteur (Core team)
 - refuse toute evolution
 - changement de licence
 - disparition de l'auteur

Les Risques liés à un projet Open Sources

- Risques liés au code source
 - gestionnaire de source vide ou en retard par rapport à la version binaire
 - production d'un exécutable impossible à partir des sources
- Risques liés au business
 - apparition d'une version entreprise
 - dépôt de marque « trademark » du projet

Exemple de projet Open Source ayant obtenu une certification ou Qualification

Netfilter

- ✓ La cible de sécurité
- ✓ Le guide de configuration
- ✓ Le rapport de certification CSPN effectué par le CESTI (scté OPPIDA) validé par l'ANSSI

EdenWall (en cours)

EAL3+

Conclusion

Pour la communauté : une démarche de développement de qualité de l'expression des besoins au déploiement

Un nouveau rôle pour les clients et les SSLL pour le développement de la confiance dans les logiciels libre

Un marché en devenir pour le logiciel libre ?

Questions / Réponses