

Annexe au CCTP Démarche ISP

MP 29-06

- **Acheteur :**

Agence de services et de paiement (ASP)
2, rue du Maupas
87040 LIMOGES cedex 1

Sommaire

Article 1.	Présentation de l'ISP	3
Article 2.	Les produits éligibles à l'ISP	3
Article 3.	L'intégration de l'ISP dans la méthode agile	4
Article 4.	Les nouveaux rôles agiles de l'ISP	4
Article 5.	Les outils mis à disposition (ASP)	5
Article 6.	Pilotage de l'ISP	6
Article 7.	Notice de la nomenclature ISP	7
Article 8.	Liste des mesures produit du socle de sécurité	7

Article 1. Présentation de l'ISP

L'ISP, pour Intégration de la Sécurité dans les Projets, est l'un des éléments fondamentaux de l'approche "security by design". Elle permet d'anticiper les besoins de sécurité et de protéger les entités contre les principaux risques qu'elles pourraient encourir dans le cadre de leurs activités numériques. En ce qu'il concerne l'application de cette méthodologie au sein de l'Agence de Services et de Paiement, l'objectif premier est de formaliser des règles liées aux développements applicatifs.

Ce principe est notamment illustré dans le Politique de Sécurité des Systèmes d'Information (PSSI) (EXG_PROJ_01) de l'ASP et dans la stratégie d'homologation du Référentiel RGS (Principe 0).

Les objectifs pour l'ASP sont :

- formaliser une démarche de développement applicatif sécurisé commune à l'ensemble des produits,
- piloter le niveau de sécurité des produits et sa progression,
- capitaliser sur les expériences des produits pour en faire bénéficier la communauté,
- initier une démarche vers le DevSecOps.

Le document qui suit vise à présenter de manière synthétique la démarche ISP ainsi que les outils mis à disposition des équipes.

Cette démarche doit être transparente pour les équipes produits, pour ce faire elle s'intègre parfaitement dans les rituels de la méthodologie « Agile ».

Le pilotage du projet ISP est à la main du Service Cybersécurité, Conformité et Réseaux (SCCR) de l'Agence. Les acteurs opérationnels du projet sont les équipes produits organisées en Lignes Produit.

Article 2. Les produits éligibles à l'ISP

Les produits éligibles à l'ISP doivent :

- être développés par l'Agence (interne ou TMA),
- respecter la méthodologie « Agile »,
- être pilotés dans JIRA.

Ne sont pas éligibles :

- les progiciels externes,
- les produits en fin de vie.

Article 3. L'intégration de l'ISP dans la méthode agile

Opérationnellement, l'ISP se traduit par la création de deux nouveaux rôles au sein des équipes produit et de la mise à disposition d'outils permettant d'estimer les besoins en sécurité.

Cette démarche vise à être transparente dans les cycles Agiles de développement. Ainsi les nouvelles actions en lien avec la sécurité que les équipes produit devront traiter vont apparaître au niveau des backlog des produits dans JIRA Software. En plus des User Stories (US) liées aux besoins fonctionnels du métier, des US sécurité seront accessibles. Il s'agit de « Security User Story » (SUS) : elles visent à traduire les règles de sécurité applicables au produit et sont issues du socle sécurité ou des vulnérabilités détectées par les outils d'analyse.

L'ISP est un point d'étape fondamental pour passer du modèle DevOps (Development – Operations) vers le modèle DevSecOps (Development-Security-Operations). Pour mémoire le DevSecOps est une méthodologie qui vise à inclure les pratiques de sécurité dans le processus de développement et de mise en production d'applications. Dans ce cadre cela implique d'anticiper la sécurité des applications et infrastructures du projet dès sa conception et ce pendant tout son cycle de vie.

Article 4. Les nouveaux rôles agiles de l'ISP

Pour faciliter la mise en œuvre de l'ISP et accompagner les équipes projet, deux nouveaux rôles sont définis :

- pour chaque ligne produit un référent sécurité ayant une vision transverse des produits pilotés ;
- pour chaque produit, un security champion ayant une vision technique et une connaissance des pratiques de développement sécurisé.

Le Référent Sécurité :

- constitue le lien entre le SCCR et les équipes des Lignes Produits,
- **traduit les exigences réglementaires et accompagne les Security Champion** dans leur montée en compétence,
- **supervise la prise en compte des SUS** par les équipes Produit,
- s'assure du respect des politiques de sécurité.

Le Security Champion :

- promeut les **règles et bonnes pratiques SSI auprès des équipes projet**,
- **assiste le Product Owner** à la sélection des User Stories « Sécurité » et à leur priorisation,
- **accompagne les développeurs** dans la prise en compte des EUS, SUS,
- s'assure de la liaison avec les services transverses DNSI,
- **contribue à la formation et à la sensibilisation des développeurs** dans le domaine de la sécurité.

Article 5. Les outils mis à disposition (ASP)

En plus des nouveaux rôles, l'ISP met à disposition des équipes plusieurs outils pour aider au pilotage de la sécurité :

Socle de sécurité : le référentiel ISP

Le socle de sécurité ISP présente des règles issues d'une part des documentations de l'Agence et d'autre part des réglementations nationales, européennes ou internationales. Il est unique et commun à l'ensemble des produits développés par l'ASP.

Le référentiel fait l'inventaire de toutes les règles de sécurité applicables aux produits de l'Agence et issues des sources telles quels :

- Stratégie d'homologation de l'ASP,
- Politique de Sécurité des Systèmes d'Information de l'Agence,
- ISO 27001,
- Référentiel Général de Sécurité (RGS),
- Les bonnes pratiques de l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI),
- La deuxième directive « Sécurité des réseaux et de l'information » (dite « directive NIS2 »),
- Etc.

Les règles de sécurité sont classées en 9 catégories :

- Données,
- DevSec,
- Identity & Access Management (IAM),
- Surveillance.

Cette analyse permet de choisir les US sécurité qui sont applicables pour le produit, de les prioriser et de générer les tickets Jira ainsi que les fiches confluence associées. Chaque SUS est identifiée par une nomenclature propre composée d'un trigramme indiquant sa catégorie et d'un numéro de série.

Les tickets intègrent le backlog du produit et sont traités au même titre que les US métier. La création des SUS est à la main des équipes « Produit ».

MonServiceSécurisé de l'ANSSI

URL : <https://monservicesecurise.cyber.gouv.fr/>

La revue du référentiel se fait dans le cadre du tableau de bord mis à disposition par l'Agence de Sécurité des Systèmes d'Information auprès de la sphère des administrations publiques.

L'administration fonctionnelle et la gestion des habilitations de MonServiceSécurisé sont assurées par le SCCR.

Le tableau de bord permet de répertorier l'ensemble des SI de l'Agence ayant intégré la démarche ISP, de réaliser les revues de conformité au socle de sécurité et d'établir les feuilles de route de mise en conformité annuelles.

Revues annuelles de conformité ISP

Chaque Ligne Produit présentée annuelle pour chacun de ses produits :

- Le taux de conformité au socle et le score cyber associé (obtenu via MonServiceSécurisé) ;
- La feuille de route de mise en conformité pour l'année N.

Les livrables (revues de conformité et feuilles de routes annuelles établies) sont communiqués au Responsable de Sécurité des Systèmes d'Information de l'Agence

Les outils d'analyse de la sécurité

Outre l'étude du socle de sécurité, les produits doivent suivre les analyses sécurité de type SAST (Test de sécurité des applications statiques) ; chaque vulnérabilité détectée donnera lieu à une SUS corrective. Cette dernière étant propre à chaque produit, il relève de la responsabilité du Security Champion la rédaction de l'US et de son intégration dans le backlog pour traitement. Une SUS du socle de sécurité peut être utilisée si elle correspond à la correction de la vulnérabilité détectée.

Test de sécurité des applications statiques (Static application security testing, SAST)

Ce test détecte les vulnérabilités des applications en analysant le code source, le code d'octets ou les binaires d'une application. En analysant les modèles de code, les flux de contrôle et les flux de données au sein d'une application, l'analyse SAST peut identifier une série de failles sans exécuter le code.

Exemple outil SAST : Checkmarx, Sonarqube Advanced

Article 6. Pilotage de l'ISP

La démarche ISP doit être portée par les équipes produit, cela transpose le principe de « security by design » qui implique le portage des mesures sécurité spécifiques à chaque sous-SI par les équipes qui conçoivent ce SI. Néanmoins le service Cybersécurité, Conformité et Réseaux, garant de l'ISP, accompagne les équipes produit sur la conception des outils, l'application des différentes règles sécurité, ainsi que la mise à jour du socle de sécurité à respecter, et assure le pilotage du projet ISP à l'échelle de l'Agence.

La comitologie

La revue de la conformité pour chaque produit est réalisée de façon annuelle. Cette revue prend forme d'un point bilatéral entre le SCCR et la Ligne Produit représentée à minima par le(s) Réfèrent(s) Sécurité et les Security Champions.

Article 7. Notice de la nomenclature ISP

Analyse de la composition des logiciels (SCA)

L'analyse de la composition des logiciels (SCA) est un outil DevSecOps permettant d'identifier ces morceaux de code externe. Le SCA peut être utilisé pour suivre les composants open-source, trouver la vulnérabilité et gérer les licences des logiciels.

Exemple outil : Trivy.

Catégorisation des SUS et numérotation :

Dans l'objectif de classifier et référencer les SUS, chaque règle issue du socle de sécurité ISP possède une nomenclature propre défini telle que : catégorie + numéro de la règle.

Les codes catégories sont les suivants :

- Données : [DAT]
- DevSec : [DSC]
- Identity & Access Management : [IAM]
- Surveillance : [SUR]

Les sources sont :

- la réglementation en vigueur (qu'elle relève de procédures internes, de réglementations nationales ou européennes) ;
- les bonnes pratiques en vigueur (notamment issues des recommandations ANSSI) ;
- les vulnérabilités connues ayant fait l'objet d'une publication ;
- les consignes du SCCR.

Article 8. Liste des mesures produit du socle de sécurité

Intitulé de la mesure	Catégorie	Criticité
DAT-1 Anonymiser et masquer les données en hors-production	Protection	
DAT-2 Tracer toutes les actions sur les données selon AIPD	Protection	
DAT-3 S'assurer qu'aucune donnée sensible n'est rendue publique	Protection	
DAT-4 Chiffrer les données confidentielles et stratégiques stockées en dehors des serveurs ASP	Protection	

ANNEXE Démarche ISP

DSC-1 Utilisation de procédures stockées pour les requêtes	Protection	P1
DSC-10 Tester et sécuriser les API (si appel API en direct, hors API Manager)	Protection	
DSC-11 Ne pas se baser sur les entrées utilisateur pour appeler des fichiers système	Protection	
DSC-12 Utiliser des identifiants uniques pour les ressources (UUID)	Protection	
DSC-13 Contrôler les fichiers déposés (liste blanche des extensions, type MIME)	Défense	P1
DSC-14 Utilisation des sécurités intégrées dans les frameworks	Protection	P1
DSC-15 Réaliser un scan antivirus des fichiers uploadés avant téléchargement sur le serveur	Protection	P1
DSC-16 Désactiver le traitement des entités XML externes (XXE)	Protection	
DSC-17 Supprimer le code caché et les vulnérabilités de type "bombes logiques" / "temporelles" ou "easter egg"	Protection	
DSC-18 Empêcher la navigation dans l'arborescence du système (Path Traversal)	Protection	P1
DSC-2 Sécurisation des secrets applicatifs	Protection	P1
DSC-3 Contrôle systématique des entrées utilisateurs (ne pas interpréter les caractères spéciaux pouvant être rajoutés)	Protection	P1
DSC-4 Valider les entrées provenant de sources externes	Protection	
DSC-5 Définir les pages d'erreurs génériques (elles ne doivent pas révéler de stack trace)	Protection	P1

ANNEXE Démarche ISP

DSC-6 Mise en place de mesures anti-CSRF	Protection	P1
DSC-7 Respecter le swagger	Protection	
DSC-8 Créer uniquement des cookies sécurisés (attributs http only et secure)	Protection	
DSC-9 Utilisation de l'API Manager	Protection	P1
IAM-1 Limiter les droits d'accès au strict besoin métier	Protection	
IAM-2 Mise à jour des droits utilisateurs	Protection	P1
IAM-3 Réaliser un contrôle périodique des accès	Protection	
IAM-4 Appliquer une politique de mot de passe conforme à la PSSI de l'Agence	Protection	
IAM-5 Application de la MFA	Protection	
IAM-6 Vérifier systématiquement le cookie de session (cloisonnement des profils et utilisateurs)	Protection	P1
IAM-7 Révoquer le cookie de session	Protection	
IAM-8 Protection des données de connexion	Protection	
IAM-9 Protection anti brute force	Résilience	
SUR-1 Messages de sensibilisation à destination des utilisateurs (être en capacité d'afficher un message au niveau de la page d'accueil et/ou mire de connexion)	Gouvernance	

ANNEXE Démarche ISP

SUR-2 Exploitation des LOG (puit de logs)	Gouvernance	P1
---	-------------	----