TUNISIA FIRST - Fiscal Reform for a Strong Tunisia

Rapport de cadrage pour la mise en œuvre de la plateforme UXP pour le compte du ministère des finances

USAID | TUNISIA
FROM THE AMERICAN PEOPLE

Table des matières

1. Introduction

Réalisé dans le cadre du projet FIRST - Fiscal Reform for a Strong Tunisia, ce rapport résume l'évaluation et les recommandations de la phase de cadrage du projet d'implémentation technique de la plateforme d'interopérabilité et d'échange de données UXP pour le compte du ministère des finances en Tunisie.

Le but de ce rapport est de fournir un plan provisoire de la seconde phase, concernant la mise en œuvre d'un pilote du projet, comprenant l'évaluation des ressources nécessaires, un calendrier et l'existence des prérequis chez les organisations participantes.

Ce rapport s'est basé sur les informations collectées lors d'une série de réunions et visites menées en Juillet 2018 entre des représentants de l'éditeur Cybernetica AS, du projet FIRST et des institutions gouvernementales participantes à la mise en œuvre d'un pilote du projet. En outre, les estimations citées dans ce rapport sont basées sur l'expérience de Cybernetica avec des projets d'implémentation des plateformes gouvernementales d'interopérabilité dans d'autres pays.

2. Abréviations

ANCE

Agence Nationale de Certification Electronique (Tuntrust)

ANSI

Agence Nationale de la Sécurité Informatique

ATTT

Agence Technique des Transports Terrestres

CA

Certification Authority

CIMF

Centre Informatique du Ministère des Finances

CNAM

Caisse Nationale d'Assurance Maladie

CNSS

Caisse Nationale de Sécurité Sociale

CPF

Conservation de la Propriété Foncière

CPU

Unité Centrale de traitement (Microprocesseur)

DGCPR
Direction Générale de la Comptabilité Publique et du Recouvrement

DGD
Direction Générale des Douanes

DGI
Direction Générale des Impôts

FIRST
Fiscal Reform for a Strong Tunisia

HSM
Hardware Security Module (Module de sécurité matériel)

HTTP
HyperText Transfer Protocol

INNORPI
Institut National de la Normalisation et de la Propriété Industrielle

MoF
Ministère des Finances

OCSP
Online Certificate Status Protocol

PIN
Personal Identification Number

PKI
Public Key Infrastructure

RA
Registration Authority

RAM
Random-Access Memory

RISC
Reduced Instruction Set Computer

RNIA
Réseau National Intégré de l'Administration

SOAP
Simple Object Access Protocol

TLS

Transport Layer Security

TTN

Tunisie TradeNet

UXP

Unified Exchange Platform

WSDL

Web Services Description Language

XML

Extensible Markup Language

3. Contexte

Malgré les grandes attentes depuis la transition paisible suivant les élections de 2014 en Tunisie, plusieurs problèmes structurels qui ont historiquement bloqué la croissance économique ont fait surface. 5 ans de partenariat avec le gouvernement des Etats-Unis depuis 2012 ont aidé à améliorer la politique fiscale, les recettes de l'administration et la gestion des finances publiques en Tunisie. En vue d'éviter de futures crises, un système fiscal réformé nécessitera des lois qui soient simples, justes et transparentes ainsi que des procédures généralisées qui réduisent les coûts de la conformité. Il faut aussi adopter des mesures qui élargissent l'assiette fiscale, réduisent les dépenses fiscales et rationalisent les impôts sur les revenus, tout en se concentrant davantage sur la taxe sur la valeur ajoutée.

L'objectif du projet "Fiscal Reform for a Strong Tunisia" (FIRST) est de fournir de l'assistance technique et un renforcement de capacité aux institutions principales du Gouvernement Tunisien, en particulier au ministère des finances (MoF) en vue de soutenir les fondations fiscales pour une croissance inclusive et pérenne. FIRST assistera le MoF dans sa capacité de formuler des politiques fiscales rationnelles, prédictibles et justes. Le projet va aussi accompagner le MoF dans la modernisation de l'administration fiscale et le renforcement de sa capacité à remplir sa tâche de recouvrement des recettes d'une manière efficace, efficiente et transparente.

Dans le cadre des activités du projet FIRST, des consultants de l'éditeur Cybernetica AS ont mené en juillet 2018 en Tunisie, une mission de cadrage relative à la mise en œuvre de la plateforme 'Unified eXchange Platform' (UXP) pour le compte du ministère des finances.

UXP est une plateforme d'échange de données dont l'efficacité est prouvée ; elle peut fournir un accès sécurisé et en temps réel à toutes les bases des données connectées des multiples organisations participantes, ce qui favorisera la réingénierie des processus métier, les flux de travail en général, et appuiera l'amélioration du service client à l'aide d'un accès rapide aux informations du contribuable. La mission de cadrage a permis d'identifier le nombre d'organisations intéressées par le projet, d'évaluer les besoins des organisations participantes et de recenser les infrastructures informatiques existantes dans toutes ces organisations. Toutes les informations obtenues pendant cette mission sont partagées dans ce rapport dont la version initiale a été préparée par Cybernetica AS.

4. Participants

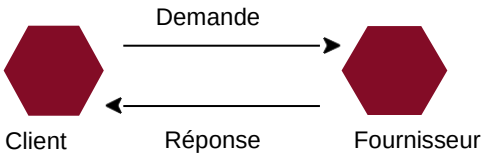
Le projet FIRST a un objectif assez vaste qui nécessite la coopération entre plusieurs ministères. Initialement, seulement un nombre précis d'institutions gouvernementales sera connecté via une plateforme d'interopérabilité dans le cadre de la première phase de mise en œuvre. Les institutions et registres suivants participeront à la première phase du projet :

- Le Centre Informatique du Ministère des Finances (CIMF) qui héberge notamment les systèmes d'information et bases de données utilisées par :
  - La Direction Générale des Impôts (DGI)
  - La Direction Générale de la Comptabilité Publique et du Recouvrement (DGCPR)
- La Direction Générale des Douanes (DGD)
- Le Registre de Commerce, hébergé et géré par l'Institut National de Normalisation et de Propriété Industrielle (INNORPI)
- L'Agence Technique des Transports Terrestres (ATTT)
- La Caisse Nationale d'Assurance Maladie (CNAM)
- La Caisse Nationale de Sécurité Sociale (CNSS)
- La Conservation de la Propriété Foncière (CPF)

En outre, l'Agence Nationale de Certification Electronique (tuntrust ou ANCE) fournira des services externes nécessaires pour l'UXP, comprenant la délivrance de certificats et l'horodatage.

5. Services

Dans l'UXP, l'échange des données est conçu comme étant un service fourni par une organisation (fournisseur) à une autre organisation (client). Sur le plan technique, le client doit déclencher l'échange en envoyant une demande au fournisseur. Ce dernier prend alors en charge la demande et fournit une réponse au client.



L'information peut passer du client au fournisseur du service ("pushing" ou "soumission" des données), ou bien du fournisseur au client ("pulling" ou "demande" des données).

Pour la première phase du projet, un nombre bien précis de services a été identifié. Les services ont été sélectionnés afin de répondre aux critères suivants :

1. Les services doivent être simples.
2. Les services doivent être ou bien déjà existants, ou bien alors simples à réaliser.
3. Les informations nécessaires pour les services doivent déjà exister sous forme numérique dans une base de données d'une organisation participante.
4. Les services doivent immédiatement être utiles pour une organisation participante.

Les services listés dans le Tableau 1 ont été sélectionnés pour la première phase du projet.

D'autres services pourront être sélectionnés par les institutions participantes en coordination avec le projet FIRST.

Tableau 1. Aperçu des services

Référence	Clients	Fournisseur	Brève description
MoF1	INNORPI, ATTT, CNAM, DGD	MoF	Situation fiscale du contribuable par le matricule fiscal (existant)
MoF2	INNORPI, ATTT, CNAM, DGD	MoF	Identité du contribuable par le matricule fiscal (existant)
MoF3	INNORPI, ATTT, CNAM, DGD	MoF	Dernière déclaration du contribuable par le matricule fiscal (existant)
MoF4	INNORPI, CNSS, DGD	MoF	Informations détaillées du contribuable par le matricule fiscal
MoF5	CNSS	MoF	Notification des changements apportés auprès de la CNSS
MoF6	CPF	MoF	Détails du contrat par référence du contrat
MoF7	CPF	MoF	Informations sur une personne par le numéro de la CIN
INNORPI1	MoF	INNORPI	Informations sur une société par le matricule fiscal
INNORPI2	MoF	INNORPI	La liste des sociétés gérées par numéro de carte d'identité ou matricule fiscal
ATTT1	MoF	ATTT	Les caractéristiques d'un véhicule à partir de l'immatriculation de celui-ci.
ATTT2	MoF	ATTT	Liste des véhicules par matricule fiscal ou numéro de CIN du propriétaire
CNAM1	MoF	CNAM	Les informations du fournisseur des services de santé par CIN et année ou par matricule fiscal et année
CNSS1	MoF	CNSS	Notification des changements apportés auprès du MoF
DGD1	MoF	DGD	Notification des changements apportés auprès du MoF
CPF1	MoF	CPF	liste des propriétaires inscrits dans la base CPF avec le code unique du propriétaire
CPF2	MoF	CPF	Liste des titres fonciers des biens relatifs à la personne à partir du code unique
CPF3	MoF	CPF	Caractéristiques d'un bien immobilier à partir d'un code de propriété

Selon le CIMF, les services MoF1, MoF2 and MoF3 existent déjà, mais doivent être actualisés. Plusieurs autres participants sont intéressés par l'utilisation de ces services selon la DGI.

Le service MoF4 est nécessaire pour solliciter les informations détaillées d'un contribuable de la part de la DGI. Ce service n'existe pas actuellement et doit être approuvé avant son développement.

Le service MoF5 est nécessaire pour la CNSS en vue d'informer le MoF des changements saisis dans le système d'information de la CNSS. C'est comme si c'était la contrepartie au service CNSS1 qui notifie la CNSS des changements enregistrés dans le système d'information du MoF. Il est impératif de noter que ce service peut être développé d'une manière à ce qu'il ne soit pas spécifique à la CNSS. Par exemple, l'implémentation du service peut utiliser l'en-tête du client UXP en vue de déterminer qui a envoyé la demande. Il faut noter que seulement les en-têtes vérifiés par UXP doivent être utilisés à cette fin alors que quelques parties du message peuvent arbitrairement être changées par le client. Ce service n'existe pas encore.
Les services MoF6 et MoF7 permettent à la CPF de valider les documents soumis. Ces services n'existent pas encore.

Les services INNORPI1 et INNORPI2 reproduisent la fonctionnalité disponible à travers le portail du registre du commerce. Malgré l'inexistence de ces services, les informations requises sont disponibles et accessibles via le portail.

Les services ATTT1 et ATTT2 permettent au MoF d'obtenir des informations sur les véhicules des personnes et des sociétés. Ces services n'existent pas encore.

Le service CNAM1 permet à la DGI de demander des informations sur le fournisseur des services de santé stockées dans le système d'information de la CNAM. Ce service n'existe pas encore.

Les services CNSS1 et DGD1 permettent au MoF de notifier la CNSS et la DGD des changements dans les informations stockées par le MoF. Ceci permettra à la CNSS et à la DGD d'avoir les informations actualisées de la part du MoF par le biais des services du MoF.

Les services CPF1, CPF2 et CPF3 permettent d'obtenir des informations sur les propriétés d'une entité en trois étapes. CPF1 aide à identifier un code interne fourni par la CPF à une entité en utilisant une partie du nom de cette entité. CPF2 permet de lister les propriétés de cette entité en utilisant le code obtenu de CPF1. CPF3 permet d'obtenir des informations détaillées sur chaque propriété séparément. Ces services n'existent pas encore.

Tableau 2. L'utilisation des services

	MoF	**INNORPI**	**ATTT**	**CNAM**	**CNSS**	**DGD**	**CPF**
MoF1		X	X	X		X	
MoF2		X	X	X		X	
MoF3		X	X	X		X	
MoF4		X			X	X	

MoF5					X		
MoF6							X
MoF7							X
CNAM1	X						
CNSS1	X						
CPF1	X						
CPF2	X						
CPF3	X						
INNORPI1	X						
INNORPI2	X						
ATTT1	X						
ATTT2	X						
DGD1	X						

Tableau 3. Estimation des efforts de développement des services

Réf	**Développé par**	**Estimation de l'institution**	**Notes**
MoF1	MoF	Existe	Peut nécessiter de la maintenance de la part du CIMF
MoF2	MoF	Existe	Peut nécessiter de la maintenance de la part du CIMF
MoF3	MoF	Existe	Peut nécessiter de la maintenance de la part du CIMF
MoF4	MoF	1 semaine	A développer par le CIMF
MoF5	MoF	1 semaine	A développer par le CIMF
MoF6	MoF	1 semaine	A développer par le CIMF

MoF7	MoF	1 semaine	A développer par le CIMF
CNAM 1	CNAM	2 semaines	A développer par la CNAM (2 Développeurs)
CNSS1	CNSS	2 semaines	A développer par la CNSS (1-2 Développeurs)
INNORPI 1	INNORPI		A développer par un sous-traitant
INNORPI 2	INNORPI		A développer par un sous-traitant
ATTT 1	ATTT		Pas de développeurs SOAP internes. l'ATTT n'est pas encore connectée au RNIA
ATTT2	ATTT		Pas de développeurs SOAP internes. l'ATTT n'est pas encore connectée au RNIA
DGD1	DGD		1 seul développeur de Web Services, manque en ressources humaines
CPF1	CPF	2 mois (3 services)	A développer par la CPF
CPF2	CPF	2 mois (3 services)	A développer par la CPF
CPF3	CPF	2 mois (3 services)	A développer par la CPF

6. Réseau sous-jacent

UXP doit être déployé sur un réseau qui connecte toutes les institutions participantes, l'autorité gouvernante, les services OCSP de l'autorité de certification et les services d'horodatage. Ce réseau peut être l'Internet public ou un intranet privé.

Pendant les discussions préliminaires, il a été suggéré que la plateforme UXP soit déployée en Tunisie sur le réseau intranet gouvernemental, RNIA, au lieu d'Internet. Cette section a pour but de comparer ces deux alternatives.

Confidentialité

UXP offre un canal sécurisé et crypté (TLS) pour les organisations participantes qui s'échangent des messages. Ce canal est protégé par des algorithmes cryptographiques standards et est conçu pour permettre une utilisation sécurisée sur les réseaux publics. Les messages sont directement transmis entre deux institutions qui communiquent ensemble. Les autres institutions (ou nœuds) connectées au même réseau ne peuvent pas décrypter les messages en transit entre un serveur de sécurité et un autre.

Il ne devrait y avoir aucune différence en termes de garanties de confidentialité entre l'utilisation de la plateforme UXP sur le réseau Internet public ou sur le RNIA.

Intégrité

Le canal sécurisé TLS entre les serveurs de sécurité garantit l'intégrité des messages en transit. En outre, tous les messages transmis via UXP sont signés par les organisations émettrices, ce qui constitue une preuve à long terme d'intégrité et de validité.

Il ne devrait y avoir aucune différence en matière de garanties d'intégrité entre l'utilisation de la plateforme UXP sur le réseau Internet public ou sur le RNIA.

Disponibilité

UXP fonctionne comme un système décentralisé lors de la transmission des messages, ce qui permet d'éviter des blocages significatifs en termes de débit et de disponibilité. Le Clustering de toutes les composantes d'UXP est aussi supporté, ce qui améliore davantage les garanties de disponibilité. Pour qu'un service soit indisponible, un événement de ceux qui suivent doit avoir lieu :

- Perte de la connectivité entre le serveur de sécurité et le réseau. La probabilité d'un cas pareil dépend directement de la robustesse du réseau et des connexions à ce réseau. Les centres de données ont la plupart du temps plusieurs connexions redondantes au réseau internet public et au réseau RNIA, ce qui réduit le risque de perte de la connectivité entre le serveur de sécurité et ces connexions. La fiabilité des réseaux eux-mêmes ne peut être estimée dans ce rapport.

- Perte de la connectivité entre le serveur de sécurité et un service ou un client. Tant que des connexions pareilles n'existent que sur les réseaux internes des organisations participantes, le risque ne dépend pas du réseau utilisé pour se connecter aux serveurs de sécurité. Il ne devrait y avoir aucune différence entre le réseau RNIA et Internet.

- Défaillance d'un service ou d'un client. Tant que les services et les clients d'une organisation ne se connectent que sur des serveurs de sécurité hébergés par l'organisation sur le réseau interne de celle-ci, ce risque ne dépend pas du réseau utilisé pour la connexion des serveurs de sécurité. Le serveur de sécurité d'UXP ne doit permettre que les messages autorisés et authentifiés, en vue de protéger les services du rejet des attaques d'un service par des agents non autorisés. Le rejet des attaques des services contre un service n'est potentiellement possible que par les organisations autorisées à avoir accès au service. Il ne devrait y avoir aucune différence entre le réseau RNIA et le réseau internet.

- Panne du serveur de sécurité. Quel que soit le réseau utilisé, tous les serveurs de sécurité doivent être protégés par des pare-feu configurés selon les exigences spécifiées dans les documents relatifs au serveur de sécurité d'UXP. Il est possible de réaliser des attaques DoS (Denial of Service, attaques par déni de service) contre les serveurs de sécurité individuels par des acteurs connectés au même réseau. L'impact d'une attaque pareille s'atténue avec une conception décentralisée d'UXP. Une attaque contre un serveur de sécurité ne pourra influencer que les services et clients d'une organisation exploitant directement ledit serveur de sécurité. Puisque le RNIA est seulement accessible aux organisations gouvernementales

approuvées, ceci doit effectivement limiter le nombre potentiel des attaquants, comparé au réseau public internet.

- Mauvaise configuration du serveur de sécurité UXP, du service ou du client. Il ne devrait y avoir aucune différence en termes de risque entre le réseau RNIA et le réseau Internet.
- Une indisponibilité de longue durée du serveur de registre UXP, du protocole OCSP ou les services d'horodatage. Il est possible d'impacter la disponibilité des services sur UXP en attaquant les composantes utilisées par tous les participants. UXP est conçu d'une façon à réduire l'impact d'attaques pareilles. Par exemple, UXP avec la configuration recommandée est robuste contre les pannes de courte durée de l'un desdits services. Les serveurs de sécurité réduisent aussi le nombre des demandes envoyées au serveur de registre UXP, OCSP et les services d'horodatage, continuent de fonctionner normalement même si quelques demandes transitent. Pour aboutir, une attaque sur ces composantes doit complètement les désactiver pour une longue période, en donnant aux administrateurs le temps de réagir. Puisque le RNIA est seulement accessible par les organisations gouvernementales approuvées, il devrait efficacement limiter le nombre des attaquants potentiels, comparé au réseau internet.

Extension

UXP est configuré pour se connecter à un nombre vaste d'organisations pour permettre l'échange des données entre elles. Pour réaliser les objectifs du gouvernement Tunisien, un grand nombre d'organisations doit être connecté à UXP en plus des organisations qui ont participé à la phase pilote. Les organisations peuvent ne pas être toutes connectées sur RNIA, alors qu'elles sont probablement toutes connectées à Internet. Même parmi les organisations qui ont approuvé de participer à la phase initiale du projet, il y a une organisation (ATTT) qui n'est pas encore connectée à RNIA et n'a pas une information précise concernant quand elle le sera. En tant que tel, l'utilisation du réseau RNIA au lieu d'Internet peut limiter les possibilités d'extension d'UXP à d'autres organisations nécessaires pour atteindre les objectifs du projet.

En résumé, on peut conclure que lors de l'utilisation d'UXP :

- Il n'y a aucune différence entre le RNIA et Internet en termes de confidentialité ;
- Il n'y a aucune différence significative entre le RNIA et Internet en termes d'intégrité ;
- Il y a des avantages dans l'utilisation du RNIA comparé à Internet en termes de disponibilité en cas de certaines attaques contre UXP ;
- Il y a des risques importants liés au réseau RNIA en termes d'extension du périmètre du projet à d'autres organisations dans le cadre de la réalisation des objectifs de haut niveau du projet.

7. Matériel nécessaire pour les participants

Afin de rejoindre la plateforme UXP, chaque participant doit avoir au moins ce qui suit dans chaque emplacement physique qui doit être connecté à UXP :

- Un **serveur d'application** pour fournir des services et consommer d'autres fournis par d'autres participants ;
- Un **serveur de sécurité UXP ;**
- Un **Hardware Security Module (HSM)** ou module de sécurité matériel connecté au serveur de sécurité pour un stockage sûr des clés cryptographiques privées.

Afin d'assurer la haute disponibilité, les serveurs de production doivent être redondants. Au minimum, il est recommandé d'avoir deux ensembles de serveurs redondants. S'il est nécessaire de réduire les

coûts, un HSM peut être partagé entre les serveurs de sécurité d'UXP redondants situés dans le même emplacement physique.

Dans le cas où les serveurs d'application sont hébergés dans de multiples sites physiques, les serveurs de sécurité UXP doivent être installés dans tous les sites. Ces sites nécessiteront des HSM séparés.

Il est hautement recommandé d'avoir des environnements séparés de production et de test pour UXP. L'environnement de test est utilisé pour développer, tester et valider les services, et ne doit pas être exploité dans l'échange d'informations réelles. Cet environnement n'est pas critique et ne demande pas des serveurs redondants. De plus, des jetons (token) logiciels peuvent substituer les HSM dans l'environnement de test pour réduire les coûts.

Il est impératif de noter qu'il est recommandé d'avoir un environnement de test UXP *permanent*. Ceci veut dire que les serveurs utilisés pour le test resteront actifs et ne seront pas déconnectés après certaines phases spécifiques du projet. Ceci est nécessaire pour permettre une intégration sûre de nouvelles organisations dans un environnement déjà existant.

Tableau 4. Ensemble de serveurs et équipements recommandés aux participants

Site	Instance	Serveurs d'application	Serveurs de sécurité UXP	HSMs
Primaire	Production	2	2	2
Primaire	Test	1	1	0
Supplémentaire	Production	1	1	1
Supplémentaire	Test	0	0	0

Les exigences de base pour un serveur opérant en tant qu'un serveur de sécurité UXP

- Une CPU avec une architecture x86-64 et au moins deux cœurs (Cores) physiques.
- Au moins 8 GB de RAM.
- Au moins 120 GB d'espace de stockage pour les messages et les logs.
- Au moins une interface réseau.
- Un serveur avec le système d'exploitation Ubuntu 16.04.

S'il est nécessaire pour des raisons budgétaires de réduire les coûts associés au matériel requis, il est possible de suivre les étapes suivantes, listées d'une façon ascendante selon le degré d'impact estimé :

1. Partager un seul HSM entre les serveurs de sécurité du site primaire (-1 HSM). Ceci peut légèrement impacter la fiabilité.
2. Garder seulement un site physique dans le cas où plusieurs sites sont disponibles (-1 serveur d'application, -1 serveur de sécurité, -1 HSM). Ceci impacte la fiabilité.
3. Commencer avec un serveur de sécurité de production et un serveur de sécurité de test, et puis convertir le serveur de test à un deuxième serveur de production (-1 serveur de sécurité, -1 serveur d'application). Ceci réduit considérablement l'utilisabilité à long terme puisqu'il n'y aurait aucune façon sûre pour tester les nouveaux services et les nouveaux clients.
4. Garder seulement un serveur de sécurité de production (-1 serveur de sécurité, -1 serveur d'application). Ceci impacte la fiabilité.

Les configurations avec un nombre inégal de serveurs d'application et de serveurs de sécurité peuvent s'avérer utiles dans certaines circonstances :

- Si un service est simple et rapide et les attaques DoS faites par des acteurs non autorisés sont assez probables, il est mieux d'avoir multiples serveurs de sécurité

- Si un service est complexe et lent et les attaques DoS faites par des acteurs non autorisés sont peu probables, il est préférable d'avoir des serveurs d'application multiples. Dans ce cas, il est nécessaire d'avoir un équilibrage de charge (Load balancing) supplémentaire entre le serveur de sécurité UXP et le service.

L'infrastructure actuelle des participants a été évaluée pendant la mission de cadrage. Les aspects suivants ont été pris en considération pour chaque participant :

- Combien de sites physiques le participant utilise pour héberger les serveurs d'application ;
- Quels types de serveurs sont utilisés dans ces sites ;
- Si le participant utilise des serveurs virtuels ou physiques ;
- S'il y a de l'espace disponible dans les sites existants pour le matériel supplémentaire ;
- Si les connexions réseaux nécessaires sont disponibles ;
- Si le personnel est prêt à gérer le matériel nécessaire.

Prière de noter que ce rapport ne détaille pas explicitement tout l'équipement et accessoires qui pourraient être nécessaires pour installer et utiliser les composantes mentionnées, tels que le matériel de montage en rack, les câbles, les connecteurs, les claviers (PIN pads) pour les HSM, les batteries de réserve, les jetons clé (key tokens), etc. Il est assumé que de tels accessoires seront acquis avec les composantes listées lorsque ceci s'avère nécessaire.

7.1. MoF et CIMF

Le CIMF sera l'autorité gouvernante de l'instance UXP en Tunisie. De ce fait, le CIMF nécessite des serveurs supplémentaires qui ne sont pas requis pour les autres participants. Puisque le CIMF est aussi une organisation participante, les mêmes HSM peuvent être exploités pour des serveurs UXP d'enregistrement et de sécurité, et les mêmes serveurs de sécurité UXP peuvent être exploités dans la gestion et l'échange habituel des données.

UXP utilise les certificats PKI (Public Key Infrastructure) et un service d'horodatage externe pour fournir certaines garanties. Chaque installation nécessite au moins une autorité de certification (CA) et au moins un service d'horodatage. Pour l'environnement de production, l'ANCE agira comme une CA de base et fournira aussi des services d'horodatage. Quant à l'environnement de test, il est recommandé d'utiliser une CA et un service d'horodatage séparés hébergés par l'autorité gouvernante. Ceci réduira les coûts et le temps requis pour préparer l'environnement de test. Puisque l'environnement de test ne doit pas être utilisé pour échanger des données réelles, il y a peu d'exigences de sécurité du côté de la CA dans l'environnement de test.

Les serveurs d'application existants seront utilisés à la fois pour gérer les services de production et les services de test ainsi que des clients. Les services nécessaires s'ajouteront aux services déjà existants dans SADEC et RAFIC.

Le CIMF n'utilisera pas un deuxième site pour ce projet. Tous les serveurs seront hébergés dans le même centre des données.

Tableau 5. Les serveurs et équipements supplémentaires nécessaires pour le MoF

Serveur ou équipement	Production	Test	Configuration de chaque serveur
Serveur de registre UXP	2	1	1 CPU core, 8 GB RAM, 60 GB de stockage
Serveur de sécurité UXP	2	1	2 CPU cores, 8 GB RAM, 120 GB de stockage
Monitoring	1	0	1 CPU core, 4 GB RAM, 60 GB de stockage
CA et RA d'UXP	0	1	2 CPU cores, 8 GB RAM, 60 GB de stockage
HSM	2	0	

Le CIMF utilise des serveurs en montage rack et des serveurs Blade dans son infrastructure, les serveurs rack sont graduellement remplacés par des serveurs Blade. Il est actuellement possible d'ajouter des serveurs rack et des serveurs Blade à l'infrastructure actuelle, mais le CIMF préfère des serveurs Blade.

Le CIMF utilise des serveurs physiques dédiés et la virtualisation avec VMWare, avec de nouveaux serveurs virtualisés. Vu que le CIMF est en phase de migration des serveurs physiques aux serveurs virtuels, il est recommandé d'utiliser des serveurs virtuels pour les serveurs UXP. Il faut aussi noter qu'à part les serveurs physiques, il faut acquérir des licences VMWare.

Le Tableau 6 résume les ressources de virtualisation supplémentaires nécessaires pour gérer les serveurs listés dans le Tableau 5.

Tableau 6. Les ressources de virtualisation nécessaires

Ressource	Quantité
CPU Cores	12 cores (4 x 1 core, 4 x 2 cores)
RAM	60 GB (7 x 8 GB, 1 x 4 GB)
Espace de stockage minimum	660 GB (5 x 60 GB, 3 x 120 GB)

Tableau 7. Matériel supplémentaire requis (non virtuel)

Élément	Nombre
HSM	2

7.2. INNORPI

- L'INNORPI est connectée au réseau RNIA.

- L'INNORPI utilise des serveurs physiques en rack avec une distribution SUSE Linux.
- L'INNORPI a des serveurs d'application existants pour la production et le test.

Actuellement, l'INNORPI n'a qu'un seul administrateur. Même si c'est suffisant pour installer et gérer un serveur de sécurité UXP, ceci pose un risque opérationnel si l'administrateur n'est pas disponible pour une raison ou une autre. L'option à long-terme pour l'INNORPI est de recruter au moins un deuxième administrateur, mais les ressources pour une telle solution peuvent manquer. Il est recommandé que l'INNORPI sélectionne au moins une autre personne qualifiée qui participera à la formation sur UXP, même si cette personne n'est pas un administrateur de serveur.

Tableau 8. Matériel supplémentaire nécessaire pour l'INNORPI

Serveur	Production	Test	Configuration de chaque serveur
Serveur de sécurité UXP	2	1	2 CPU cores, 8 GB RAM, 120 GB de stockage
HSM	2	0	

7.3. ATTT

- ATTT n'est pas connectée au réseau gouvernemental RNIA. L'ATTT a déclaré avoir demandé d'être connectée au RNIA deux mois avant la mission de cadrage, mais il n'y a pas encore eu de retour sur ce point. Puisque la plateforme UXP est initialement supposée être déployée sur RNIA, ceci pose un problème qui doit être résolu. Les solutions possibles sont les suivantes :
  - La plateforme est déployée sur le réseau internet. Ceci a été bien expliqué dans la section Section 6.
  - L'ATTT est connectée au RNIA le plutôt possible. Ceci peut demander un support supplémentaire de la part du MoF et du projet FIRST pour le faciliter, y compris l'obtention de l'accord et le matériel réseau requis. Ce rapport n'offre aucune évaluation de cette solution.
  - L'ATTT est connectée à UXP qui est déployé sur le réseau RNIA à travers un serveur de sécurité hébergé par le MoF. Ceci peut nécessiter l'établissement d'une connexion sécurisée entre l'ATTT et le MoF et pourrait aussi engendrer la perte de toutes les garanties fournies par UXP. Ce rapport n'offre aucune évaluation de cette solution.
- L'ATTT utilise des serveurs physiques montés en rack sous Red Hat Enterprise Linux 6.5
- L'ATTT peut fournir des serveurs virtuels pour la phase de test si nécessaire. Puisque un environnement de test permanent est conseillé, il est impératif de fournir un serveur dédié au test.
- Une demande de serveurs physiques supplémentaires a été formulée pour la phase de production. Il y a des unités rack qui sont disponibles.

Tableau 9. Matériel supplémentaire nécessaire pour l'ATTT

Serveur	Production	Test	Configuration de chaque serveur

Serveur de sécurité UXP	2	1	2 CPU cores, 8 GB RAM, 120 GB de stockage
HSM	2	0	

7.4. CNAM

- La CNAM utilise des serveurs physiques sous Linux CentOS.
- La CNAM utilise des processeurs RISC dans leur infrastructure. UXP a été créé pour une architecture x86-64 et les serveurs exécutant UXP doivent avoir des CPUs x86-64 (comme c'est le cas pour tous les autres participants).
- La CNAM peut fournir des serveurs virtuels pour la phase de test si nécessaire. Puisqu'il est recommandé d'avoir un environnement de test permanent, il est impératif de fournir un serveur dédié au test.
- Une demande de serveurs physiques supplémentaires a été formulée pour la phase de production.

Une réunion tenue le 31/08/2018 entre des représentants du projet FIRST et de la CNAM, a permis de discuter les recommandations initiales ci-dessus et de les préciser comme suit :

Pour l'environnement de test :

- *La CNAM se charge de fournir un environnement de test dédié au projet UXP tout au long de son cycle de vie,*
- *L'environnement de test sera composé de deux (2) serveurs physiques : 1 serveur UXP et 1 serveur d'application,*

Pour l'environnement de production :

- *En plus des serveurs UXP et des modules HSM, la CNAM aura besoin de 2 serveurs d'application pour héberger de manière redondante les web services et clients à développer.*

Tableau 10. Matériel supplémentaire nécessaire pour la CNAM

Dispositif	**Qté**	**Description**	**Technologie**	**Caractéristiques**
Serveur de Sécurité UXP	2	Serveur qui héberge le Package UXP	Rack	Microprocesseurs : 2 CPU cores RAM : 8 GB RAM Stockage : 120 GB
Serveur d'application	2	Serveur pour héberger les web services	Rack	Microprocesseurs : 2 CPU cores RAM : 8 GB RAM Stockage : 120 GB
HSM (Hardware Security Module)	2	Dispositif connecté au Serveur de Sécurité UXP pour le stockage sécurisé des clés cryptographiques privées.	-	-

7.5. CNSS

- La CNSS utilise des serveurs **virtuels** sous Linux CentOS.

- La CNSS possède des serveurs rack et des serveurs Blade.
- La CNSS a exprimé une préférence pour les serveurs Blade et est prête à fournir les spécifications correspondantes.
- Il y a de l'espace pour deux serveurs rack physiques si nécessaire. Ceci veut dire **qu'il pourrait ne pas y avoir assez d'espace pour les serveurs rack nécessaires** (3 serveurs et 1 HSM). Il faudrait alors penser à des serveurs Blade.
- La CNSS peut fournir des serveurs virtuels pour la phase de test si nécessaire. Puisqu'il est recommandé d'avoir un environnement de test permanent, il est impératif d'avoir un serveur dédié.

Tableau 11. Matériel supplémentaire nécessaire pour la CNSS

Serveur	Production	Test	Configuration de chaque serveur
Serveur de sécurité UXP	2	1	2 CPU cores, 8 GB RAM, 120 GB de stockage
Serveur d'application	2	0	Spécifications à obtenir de la CNSS
HSM	2	0	

7.6. DGD

- La DGD utilise actuellement des serveurs physiques rack.
- La DGD projette d'acquérir des serveurs Blade dans 6 à 8 mois à partir de Juillet 2018. La DGD continuera à utiliser à la fois les serveurs rack et Blade.
- Il est recommandé de fournir des serveurs rack pour les composantes UXP.
- Il y a 12 unités disponibles pour des serveurs supplémentaires.
- Les bases de données de test et de production sont disponibles, sur le même serveur.
- La DGD peut fournir des serveurs virtuels pour la phase de test si nécessaire. Puisqu'il est recommandé d'avoir un environnement de test permanent, il est impératif d'avoir un serveur dédié.

Tableau 12. Matériel supplémentaire nécessaire pour la DGD

Serveur	Production	Test	Configuration de chaque serveur
Serveur de sécurité UXP	2	1	2 CPU cores, 8 GB RAM, 120 GB de stockage
HSM	2	0	

7.7. CPF

- La CPF est en cours de migration du serveur physique à une plateforme virtualisée. Cette

migration est prévue d'être finalisée vers Mars ou Mai 2019.

- Le centre des données actuel utilise des serveurs rack physiques.
- Le nouveau centre des données utilisera des serveurs Blade opérant sous VMware.
- Un centre de données de secours distant sera préparé en 2019.
- Une solution intermédiaire peut être une location provisoire des serveurs rack physiques jusqu'à la finalisation de la migration et acquisition des serveurs Blade et les licences nécessaires pour la virtualisation de la plateforme en attendant que le nouveau centre des données soit disponible. De ce fait, cette section offre des estimations séparées pour les deux phases.
- Un plan de migration doit être préparé pour permettre une migration fluide vers le nouveau centre de données.
- Actuellement, il n'y a aucune base de données centralisée. Les informations sont enregistrées au niveau des 21 bureaux régionaux. Ces bureaux peuvent communiquer par le biais de web services à travers le bureau central.
    - Le serveur de sécurité UXP et les services et clients nécessaires seront déployés au bureau central. Les bureaux régionaux communiqueront avec le bureau central, et non pas directement avec UXP.

Tableau 13. Matériel supplémentaire nécessaire pour la CPF avant la migration

Serveur	**Production**	**Test**	**Configuration de chaque serveur**
Serveur de sécurité UXP	2	1	2 CPU cores, 8 GB RAM, 120 GB de stockage
HSM	2	0	

Tableau 14. Serveurs virtuels nécessaires pour la CPF après la migration

Serveur	**Production**	**Test**	**Configuration de chaque serveur**
Serveur de sécurité UXP (primaire)	2	1	2 CPU cores, 8 GB RAM, 120 GB de stockage
Serveur de sécurité UXP (secondaire)	1	0	2 CPU cores, 8 GB RAM, 120 GB de stockage

Tableau 15. Matériel supplémentaire nécessaire pour le centre de données primaire de la CPF après la migration

Ressource	**Quantité**
CPU Cores	6 cores (3 x 2 cores)
RAM	24 GB (3 x 8 GB)
Espace minimum de stockage	360 GB (3 x 120 GB)

Tableau 16. Ressources de virtualisation supplémentaires nécessaires pour le centre de données de secours de la CPF après la migration

Ressource	Quantité
CPU Cores	2 cores (1 x 2 cores)
RAM	8 GB (1 x 8 GB)
Espace minimum de stockage	120 GB (1 x 120 GB)

Tableau 17. Matériel supplémentaire nécessaire pour la CPF après la migration

Serveur	Production	Test	Remarques
HSM (primaire)	2	0	Les HSMs exploités avant la migration peuvent être utilisés à cette fin.
Serveur	**Production**	**Test**	**Remarques**
HSM (secondaire)	1	0	Un HSM supplémentaire sera nécessaire pour le centre de données de sauvegarde.

8. Formation

Cybernetica fournit des formations pour les administrateurs gérant les composantes UXP et pour les développeurs logiciels qui vont implémenter les services et les clients qui vont utiliser la plateforme UXP. Puisque toutes les organisations participantes seront appelées à gérer des serveurs de sécurité et de développer des services et des clients pour la plateforme, il est nécessaire d'organiser des formations pour les développeurs et les administrateurs de toutes les organisations participantes.

Il est souvent suffisant d'avoir 2 à 3 administrateurs de chaque organisation participante qui gèreront les installations des serveurs de sécurité UXP. Le nombre des développeurs devant être formés dépend des services spécifiques à développer. Néanmoins, un nombre de 2 à 3 développeurs par organisation est suffisant.

Une considération particulière doit être accordée au CIMF, car il a de loin le plus grand nombre de services et clients à développer. De plus, cette organisation est responsable de l'hébergement et de la gestion des composantes centrales d'UXP.

Il faut aussi considérer le fait que les employés des organisations participantes se sentent plus à l'aise avec la langue arabe ou française. Même s'il est possible de faire appel à un interprète, il y a des risques de perte de temps et de détails surtout que les participants à la formation ne pourront pas communiquer directement avec le formateur. Vu tous ces facteurs, il est recommandé de mener les formations sur deux phases séparées.

8.1. Formation des formateurs

La première phase est de *former les formateurs*. Le but de cet exercice est de trouver et former des spécialistes en informatique qui parlent couramment l'Arabe, le Français et l'Anglais. Ces derniers

recevront la formation par Cybernetica AS et seront après capables de former les autres participants. Les formateurs doivent eux-mêmes être des spécialistes en informatique compétents pour pouvoir gérer et développer les web services ou les applications exécutant ces services.

Vu le besoin d'avoir une équipe de support tunisienne compétente qui fournira la première ligne de support aux organisations participantes, les membres de l'équipe de support doivent aussi participer à la formation des formateurs.

1. Les formateurs recevront une formation approfondie. La formation insistera particulièrement sur l'assimilation des détails d'implémentation, l'analyse des problèmes potentiels et des questions relatives à la plateforme UXP, et l'introduction d' UXP aux autres.

Les critères pour tous les formateurs

1. Les formateurs doivent couramment parler l'Arabe et/ou le Français pour pouvoir former les spécialistes en informatique des autres organisations.
2. Les formateurs doivent parler couramment l'Anglais pour recevoir une formation approfondie de Cybernetica AS.
3. Les formateurs doivent être des spécialistes en informatique répondant à un profil technique requis (détails ci-dessous) pour comprendre les détails du fonctionnement des composantes UXP.
4. Les formateurs doivent être habitués au réseautage, y compris la terminologie requise, une compréhension de base des protocoles TCP/IP et HTTP et la configuration des pare-feu.
5. Les formateurs doivent maîtriser les principes de base des web services.

Critères des formateurs des administrateurs du Serveur de sécurité UXP
1. les formateurs doivent être compétents dans le domaine de gestion des serveurs exécutant les variantes des systèmes d'exploitation GNU/Linux or *nix (Serveur Ubuntu de préférence).

Critères pour les formateurs des développeurs de logiciel utilisant UXP

1. Les formateurs doivent maîtriser les langages de programmation et les plateformes utilisées pour développer des services ou des clients par les participants (des langages et des plateformes spécifiques sont indiqués dans le tableau Table 19). Il n'est pas nécessaire que tous les formateurs connaissent tous les langages et plateformes. Mais pour chaque langage et plateforme, il faut au moins un seul formateur familiarisé avec cette plateforme.
2. Les formateurs doivent maîtriser XML, XML Schema, WSDL et SOAP.

Il est prévu que le projet FIRST sélectionne les formateurs.

Il est recommandé que tous les formateurs participent à toutes les sessions de formation pour avoir une idée plus approfondie sur la plateforme ainsi que sur les outils et méthodes de développement.

Tableau 18. Programme de formation des formateurs

Jour	Format	Durée	Sujet
1	Discussion	Demi-journée	Introduction à UXP

1	Pratique	Demi-journée	Administration du serveur de sécurité UXP, partie 1 - installation et configuration initiale
2	Pratique	Journée entière	Administration du serveur de sécurité UXP, partie 2 - configuration, clients, services, sécurité et contrôle d'accès
3	Pratique	Journée entière	Administration du serveur de sécurité UXP, partie 3 - redondance, surveillance, enregistrement et diagnostics
4	Pratique	Journée entière	Le serveur de registre UXP, partie 1 - préparation au système, installation et configuration
5	Pratique	Journée entière	Le serveur de registre UXP, partie 2 -haute disponibilité, surveillance, enregistrement et diagnostics
6	Discussion	Demi-journée	Les basiques sur XML, SOAP et WSDL
6	Pratique	Demi-journée	Création des services pour UXP et développement des services en utilisant le connecteur UXP
7	Pratique	Journée entière	Développement des services et des clients en Java
8	Pratique	Journée entière	Développement des services et des clients en PHP
9	Pratique	Journée entière	Autorité d'enregistrement et CA d'UXP
10	Pratique	Journée entière	Session pratique d'intégration et d'autres sujets supplémentaires suggérés par les apprenants

La formation des formateurs peut se tenir en Tunisie ou en Estonie. Les critères des lieux de la formation sont décrits dans la Section 8.3.

Si la formation se tient en Tunisie, 2 formateurs de Cybernetica AS doivent venir en Tunisie pendant deux semaines. Le projet FIRST devra fournir les locaux appropriés pour la formation.

Si la formation est tenue en Estonie, Cybernetica AS se chargera de trouver des locaux appropriés pour la formation.

8.2. Formation des participants

Tableau 19. Formation requise par participant et nombre des apprenants

	SS	Dév. Java	Dév. PHP	Oracle 11g	RS
MoF	2-4	16	0	16	2-4
INNORPI	1-3	0	0	2-3	0
ATTT	2-3	0	0	2-3	0
CNAM	2-3	0	0	2-3	0
CNSS	2-3	2-3	0	2-5	0

DGD	0-3	0-3	0	0-3	0
CPF	2-3	2-3	2-3	0	0
Total	11-22	20-25	2-3	24-33	2-4

Explication des colonnes du tableau ci-dessus :

- SS - Administration et surveillance du Serveur de sécurité UXP. Il est recommandé que chaque organisation ait au moins 2 ou 3 employés capables de gérer le serveur de sécurité UXP.
- Dév Java. - développement des services et des clients en utilisant Java.
- Dév PHP - développement des services et des clients en utilisant PHP.
- Oracle 11g - développement des services et des clients en utilisant la base des données Oracle et Oracle Forms 11g.
- Connector - développement des services en utilisant UXP Connector.
- **RS** - administration, surveillance et Clustering du serveur de registre UXP. Il est recommandé que tous les administrateurs anglophones du serveur de registre du CIMF participent à la formation des formateurs.

En outre, tous les participants doivent participer aux sessions d'introduction--introduction à la plateforme UXP et les basiques de XML, SOAP and WSDL.

8.2.1. INNORPI

- Apache Tomcat est utilisé comme serveur d'application.
- Oracle 11g est utilisé pour le stockage des données
- Pendant la mission de cadrage, l'INNORPI a déclaré n'être capable de fournir qu'un seul administrateur du serveur de sécurité UXP.

  Il est recommandé d'avoir au moins deux personnes de l'INNNORPI pour participer à la formation, même si l'une d'entre elles n'est pas vraiment un administrateur de serveur.

- L'INNORPI a actuellement déployé des web services SOAP. Cependant, ces web services ont été développés par une agence externe de développement des logiciels. L'INNORPI n'a actuellement pas de développeurs internes de web services.

  Il est recommandé ou bien de sélectionner des développeurs externes d'une agence de développement recommandée par l'INNORPI pour participer à la formation des développeurs, ou alors de sélectionner des membres du personnel qui soient compétents en développement JAVA pour participer à la formation des développeurs pour qu'ils puissent conseiller les développeurs d'une agence externe ou, le cas échéant, développer des services et des clients eux-mêmes.

8.2.2. ATTT

- L'ATTT peut désigner des administrateurs pour la formation.
- L'ATTT utilise Oracle 11g et Oracle Forms.

- L'ATTT a actuellement 3 développeurs. Néanmoins, ils n'ont pas d'expérience dans le développement des services SOAP. L'ATTT n'a actuellement aucun service SOAP en exploitation.

  Il est recommandé que l'ATTT désigne 2-3 programmeurs disponibles pour la formation des développeurs d'UXP. Même si cette formation n'est pas suffisante pour un novice du développement des web services, elle explique comment créer des web services et des clients SOAP basiques. Pendant le développement, ces personnes peuvent requérir une aide supplémentaire.

8.2.3. CNAM

- La CNAM peut désigner des administrateurs pour la formation.
- La CNAM a des web services existants développés sous Oracle 10g et Oracle Forms 6 en interne.
- La CNAM déclare avoir les capacités nécessaires de développement des web services et des clients pour le projet. Il y a des développeurs disponibles pour la formation.

8.2.4. CNSS

- La CNSS peut désigner 2 administrateurs de serveur pour la formation.
- La CNSS utilise Oracle Forms.
- La CNSS a des services SOAP existants développés en interne sur Java, Apache Axis et IBM WebSphere. Ces services sont fournis à la CNAM et d'autres administrations. 5 développeurs sont disponibles pour la formation.

8.2.5. DGD

- La DGD utilise une base de données Oracle, PL/SQL, Oracle Forms et Java pour développer et consommer au moins quelques services.
- Il y a un serveur d'application Glassfish.
- La DGD a des web services SOAP existants pour échanger des informations avec la CNSS.
- Actuellement, il y a 5-6 ingénieurs dans le département de développement. Mais, selon la DGD, ils ne sont pas disponibles pour développer des services, car leur département est en sous-effectif.
- Il peut y avoir des problèmes de disponibilité du personnel de la DGD pour la formation et pour le projet en général à cause de la lourde charge de travail. Ce risque doit être pris en considération lors de la planification de la formation et du développement.

8.2.6. CPF

- Il y a 3 administrateurs, 3 développeurs de web services et 10 développeurs de logiciels au total. Ils sont disponibles pour la formation.
- La CPF a des services SOAP existants développés en interne avec Java et des clients développés sur PHP.

8.3. Exigences relatives aux salles de formation

La salle doit contenir assez de place pour tous les participants. Les participants doivent pouvoir entendre l'instructeur clairement et voir aussi bien le tableau que l'écran de projection.

- Un PC de bureau ou un PC portable (laptop) pour chaque participant (description détaillée ci-dessous) OU un emplacement pour les participants qui choisissent d'apporter leurs propres PC portables.
- Une connexion LAN câblée pour chaque PC.
- Un projecteur avec une entrée VGA ou HDMI, et les câbles nécessaires (la connexion au projecteur doit être accessible à l'instructeur).
- Un tableau blanc ou un tableau de papier, marqueurs et effaceur (ou brosse de tableau).

Critères des PC pour les participants

- 64-bit CPU avec VT-x (Processeurs Intel) ou bien AMD-v (processeurs AMD) activé.
- Système d'exploitation à 64-bit (Windows, OS X ou GNU/Linux) capable d'exécuter Oracle VirtualBox (version 64-bit).
- Au moins 4GB de RAM (il est recommandé d'avoir 8GB).
- Au moins 30GB d'espace disque libre.
- Un port USB accessible.

Il doit être possible de créer des machines virtuelles Ubuntu 64-bit avec au moins 2GB de RAM en utilisant VirtualBox !

Les logiciels tiers suivants doivent être installés :

- Oracle VirtualBox 5.2 (64-bit)
- Oracle Java SE Runtime Environment 8
- SmartBear SoapUI 5.4 (édition OpenSource)
- WinSCP 5.13
- La dernière version de Firefox ou de Chrome

Critères du réseau local

- Tous les ordinateurs des participants et des instructeurs doivent être connectés au même réseau local et doivent être capables de s'envoyer des paquets. La connexion doit être stable et permettre au moins 100Mbps de débit d'échange de données sur le réseau local (un réseau de 1Gbps est recommandé). La connexion par câble est extrêmement recommandée.
- Il doit y avoir 2 adresses IPv4 disponibles pour chaque participant (une pour l'hôte et une pour la machine invité). Il faut réserver 5 autres adresses IPv4 supplémentaires qui soient assignées statiquement pour utilisation par les instructeurs. Par exemple, s'il y a 16 participants, il doit y avoir 2 x 16 + 5 = 37 adresses IPv4 disponibles. 5 parmi elles doivent être statiquement assignées aux machines virtuelles utilisées par les instructeurs.
- Il est recommandé que les adresses IP des participants soient aussi affectées statiquement à leurs ordinateurs ou que le bail DHCP (DHCP lease) soit assez long pour que les adresses IP ne changent pas pendant la formation (les deux jours).

9. Support

Après le déploiement de la plateforme UXP, il est attendu que les participants soient capables de gérer les composantes de UXP en toute autonomie grâce aux compétences acquises durant la formation. Il est nécessaire d'avoir une équipe de support pour conseiller les participants sur les problèmes potentiels que les participants ne pourront pas résoudre seuls. Cybernetica AS offre support et maintenance pour UXP, mais il est recommandé d'avoir deux niveaux de support distincts.

Le but du premier niveau de support est de communiquer directement avec les participants et de fournir le conseil et le support nécessaires. L'équipe agissant au premier niveau de support doit être composée de spécialistes qui ont suivi la formation des formateurs menée par UXP puisque cette formation se focalise sur le transfert des connaissances et le travail avec d'autres participants. Cette équipe doit être capable de traiter les soucis de configuration les plus communs et répondre à des questions simples à propos d'UXP. Dans le cas où cette équipe de support rencontre un problème ou une question qu'elle est incapable de traiter, elle doit envoyer une demande de support traduite en anglais au deuxième niveau de support fourni par Cybernetica AS.

Le deuxième niveau de support est assuré par Cybernetica AS et il vise à résoudre les problèmes compliqués et répondre à des questions qui demandent des connaissances sur les détails d'implémentation d'UXP. Le deuxième niveau de support est régi par un contrat de support et de maintenance qui souvent comprend un certain nombre d'heures de support avec une option d'achat d'heures supplémentaires si nécessaire et qui spécifie un accord sur le niveau de service (SLA).

Normalement, Cybernetica AS fournit aussi des mises à jour des composantes UXP selon le contrat de maintenance. Ces mises à jour peuvent comprendre des corrections d'anomalies dans les logiciels fournis par Cybernetica AS, des améliorations des fonctionnalités existantes ou un rajout de fonctionnalités supplémentaires. Les changements spécifiques sont décrits dans le journal de modifications qui font partie du même package de mise en production.

10. Modifications recommandées pour UXP

UXP est un produit complet et prêt à l'emploi. Néanmoins, il y a des personnalisations qui peuvent être appliquées comme des add-ons ou des plug-ins pour mieux répondre aux besoins d'un client. Normalement, ceci inclut l'ajout de langues supplémentaires pour la plateforme UXP qui, par défaut, est fourni avec une interface d'utilisateur et une documentation en anglais. Aussi, d'autres modifications peuvent être appliquées selon l'accord conclu entre le client et Cybernetica AS.

Dans le cas de l'installation d'UXP en Tunisie, il est recommandé de développer une traduction française de l'interface utilisateur et de la documentation.

En outre, un profil de certificat personnalisé devra être créé, si l'ANCE / Tuntrust l'exige.

10.1. Traduction

Pour les besoins de la mission de cadrage, il a été convenu d'avoir un interprète qui assure la traduction entre l'arabe, l'anglais et le français. Pendant la mission de cadrage, il est devenu clair que malgré le fait que quelques employés des organisations participantes parlent et comprennent l'anglais, il y a aussi quelques spécialistes qui ont suivi la traduction. Ces mêmes personnes auront besoin de versions en

arabe ou en français de la documentation UXP, de l'interface utilisateur et de la formation.

La traduction en arabe de l'interface et des documents UXP sollicitera énormément d'effort de la part de Cybernetica AS pour élaborer des supports pour les langues écrites de droite à gauche et pourra retarder de manière significative la mise en œuvre du projet. Il est vivement recommandé de traduire l'interface utilisateur en français, au moins pour le moment. Ce rapport assume une traduction en français et n'évalue pas l'effort nécessaire pour mettre en œuvre une interface utilisateur en arabe.

Les web services et les clients exploitant UXP peuvent utiliser la langue arabe ou toute autre langue supportée par Unicode indépendamment de la langue de l'interface utilisateur d'UXP.

La traduction de l'interface et de la documentation est souvent faite par un partenaire local, et non pas par Cybernetica AS. Une traduction pareille exige un traducteur technique qui maîtrise la terminologie informatique relative au réseautage, web services et cryptographie.

Le support de formation est souvent traduit et personnalisé par les formateurs eux-mêmes. Il est recommandé que la documentation soit traduite et partagée avec les formateurs avant même de commencer la formation des participants et lorsque les formateurs sont encore en train de travailler sur le matériel de formation. Ceci permet aux formateurs qui ont suivi la formation sur UXP d'offrir au traducteur un support de valeur pour s'assurer de l'exactitude des termes et des explications. Ceci garantit une terminologie unifiée, exacte et pertinente pour toute la documentation et tout le support de formation.

Puisqu'il est important d'avoir une configuration correcte des composantes d'UXP pour des questions de sécurité et de fiabilité de l'échange de données, il est donc d'autant plus important que tous les administrateurs réseau et administrateurs des serveurs travaillant sur UXP soient capables de lire et comprendre pertinemment la documentation d'UXP. Ceci nécessite la traduction de tous les guides d'utilisateurs et des spécifications vers une langue qui soit très bien comprise par le personnel des organisations participantes. Les documents suivants nécessiteront une traduction :

- Guide d'installation du serveur de registre UXP (UXP-IG-RS)
- Guide d'installation et de configuration du serveur de registre UXP en haute disponibilité (UXP-IG- RSHA)
- Guide d'utilisateur du serveur de registre (UXP-UG-RS)
- Guide d'installation du serveur de sécurité UXP (UXP-IG-SS)
- Guide d'utilisateur du serveur de sécurité UXP (UXP-UG-SS)
- Paramètres du système UXP (UXP-UG-SYSPAR)
- Guide d'utilisateur de la console de signature UXP (UXP-UG-SC)
- Guide de vérification des documents signés UXP (UXP-UG-SIGDOC)
- Guide d'installation du monitoring UXP (UXP-IG-MS)
- Guide d'installation du connecteur UXP (UXP-IG-CONNECTOR)
- Guide d'utilisateur du connecteur UXP (UXP-UG-CONNECTOR)
- Guide d'installation du CRA UXP (UXP-IG-CRA)
- Guide d'utilisateur du CRA UXP (UXP-UG-CRA)
- Guide de démarrage rapide : serveur de sécurité (UXP-QSG-SS)

- Guide de démarrage rapide : Mise en œuvre des services par le connecteur UXP (UXP-QSG-CONNECTOR)
- Guide de démarrage rapide : développement des clients de services UXP (UXP-QSG-JCLIENT)

Tous les documents sont normalement envoyés pour être traduits de l'anglais en format de texte simple AsciiDoc. La version PDF des documents générés par les fichiers AsciiDoc sont aussi fournis à titre de référence. Il est prévu que les documents traduits soient retournés sous format AsciiDoc valide. Cybernetica AS génèrera alors la version PDF des documents traduits.
Les captures d'écran de l'interface d'utilisateur et toute autre illustration seront modifiées par Cybernetica AS. Les images originales en anglais seront partagées avec les traducteurs. Les captures d'écran de l'interface d'utilisateur seront mises à jour par Cybernetica quand la traduction de l'interface est finalisée. D'autres illustrations peuvent nécessiter une traduction manuelle. Il est attendu que les traducteurs fournissent des commentaires sur la manière dont ces illustrations seront traduites.

Même si l'interface d'utilisateur UXP est assez simple, il est préférable de la traduire dans la même langue de la documentation pour éviter tout problème de mécompréhension et réduire les risques de mauvaise configuration par conséquent. Les interfaces des composantes suivantes nécessitent une traduction :

- Serveur de registre UXP
- Serveur de sécurité UXP
- Connecteur UXP
- UXP CRA

Puisque la documentation réfère souvent à des détails précis sur l'interface de l'utilisateur, il est recommandé que les mêmes traducteurs travaillent sur la documentation et l'interface de l'utilisateur. Ceci est nécessaire pour éviter la confusion et la différence entre les termes utilisés pour traduire la documentation et l'interface.

11. Risques et problèmes

Cette section est consacrée aux risques liés au projet, leur impact et les solutions potentielles de Cybernetica AS en se basant sur les informations rassemblées lors des réunions avec les participants. Il peut y avoir d'autres risques liés au projet qui ne sont pas mentionnés dans cette section.

Les délais pour ce projet sont compressés.

Même si le projet est réalisable en une période de 6 mois, ceci laisserait très peu de marge pour les retards potentiels. La motivation et la hâte de réaliser ce projet sont bien palpables, mais elles demandent beaucoup d'effort de la part des différentes institutions en plus de leur charge de travail habituelle. Ceci veut dire que des retards pendant les phases de développement sont bien probables et que ceci pourrait engendrer des décalages dans les délais du projet en entier.

Il faut noter que la réussite du projet dépend en grande partie du degré de priorité que les institutions participantes lui attribuent. Quelques organisations participantes ont clairement annoncé leur manque en ressources humaines et l'indisponibilité de certaines personnes. Il est important de classer ce projet comme prioritaire pour que le personnel nécessaire soit présent aux formations, soit prêt à configurer

les composantes nécessaires et développer les services et clients requis.

Il est recommandé de :

- Souligner aux organisations participantes l'importance de ce projet et avoir leur engagement de prioriser ce projet ;
- Segmenter le projet en petites étapes avec des objectifs et des délais clairs pour les participants ;
- Rester constamment en contact avec tous les participants en vue de détecter tous les problèmes et retards potentiels assez tôt et fournir le support nécessaire ;
- Prévoir l'éventualité que les phases de développement prennent beaucoup plus de temps que prévu.

Le MoF pourrait être sollicité à fournir les critères des services aux autres participants.

Il est normalement attendu que les fournisseurs des services eux-mêmes conçoivent leurs services. Cependant, il n'est pas fréquent que les fournisseurs des services fassent usage de leurs propres services. Ce qui veut dire qu'il y aurait peut-être des confusions à comprendre quelle information est justement demandée de la part des autres participants. Afin d'éviter ceci, le MoF doit formuler clairement les services dont il a actuellement besoin, les données d'entrées et les résultats ainsi que leur utilisation par le MoF.

Si le choix se porte sur le réseau RNIA, d'autres organisations ne pourront pas avoir accès à UXP.

Bien que l'utilisation d'un intranet gouvernemental apporte en effet quelques avantages discutés dans la Section 6, ce scénario a un inconvénient majeur qu'il ne faut pas négliger : Tout nouveau partenaire d'échange de données devra d'abord se connecter au RNIA avant de pouvoir utiliser UXP. Ceci peut nécessiter plus de temps, de matériel et d'effort pour utiliser UXP. Une telle évaluation est en dehors du cadre de ce rapport.

En ce moment, il est déjà clair que parmi les sept organisations participantes dans la phase initiale, au moins l'ATTT n'est pas encore reliée au RNIA. A ce stade, il n'y a même pas de délais prévisionnels pour l'établissement de la connexion de l'ATTT au RNIA. Il n'y a pas d'indications exactes non plus sur le nombre des institutions connectées au RNIA parmi celles qui devront rejoindre UXP pour atteindre les objectifs du ministère des finances. Ce qui veut dire qu'il n'est pas possible d'estimer les délais et efforts nécessaires pour l'adhésion de nouvelles institutions si le choix se porte sur un déploiement d'UXP sur le réseau RNIA.

Il est d'autant plus important de mentionner le fait que l'utilité d'UXP ne se limite pas à ce projet. Il pourrait ultérieurement, s'avérer nécessaire que des organisations en dehors du périmètre du projet actuel doivent adhérer à UXP pour pouvoir échanger des informations avec une des autres institutions utilisant la plateforme.
Par exemple, en Estonie, la même plateforme est utilisée aussi bien pour les échanges gouvernementaux de données que pour les communications entre institutions privées et le gouvernement. Il serait difficile, voire carrément impossible, de réaliser ceci en Tunisie, si le choix se porte sur un déploiement d'UXP sur un intranet accessible uniquement pour certaines institutions.

La DGD manque de ressources humaines et peut ne pas avoir de développeurs disponibles

pour le projet.

Pendant la réunion, la DGD a maintes fois évoqué son manque en ressources humaines et la difficulté qu'elle aurait à dédier des développeurs pour la mise en œuvre des services escomptés. Même si la solution optimale pour la DGD serait probablement de recruter du personnel supplémentaire, ceci n'entre pas dans le cadre de ce projet et il faudrait envisager d'autres mesures.

Pendant la réunion, le périmètre a été réduit pour que la DGD ne développe qu'un seul service simple en vue de recevoir des notifications des modifications de la part du MoF. Ceci devra réduire la charge de développement des web services à un minimum. La DGD aura aussi besoin de développer un client qui récupère les informations de la part du MoF.

Il est recommandé de :

- Insister sur l'importance du projet UXP auprès de la DGD ;
- Faire recours, le cas échéant, à la sous-traitance pour développer les services et les clients nécessaires.

L'INNORPI a des ressources très limitées.

Au moment de la réunion, l'INNORPI avait un seul administrateur qui pourrait potentiellement gérer les serveurs de sécurité UXP. Aussi, l'INNORPI fait appel aux services d'un sous-traitant externe pour leurs besoins de développement logiciels. En général, l'INNORPI déclare avoir des ressources très limitées. Même si l'INNORPI semble très intéressée par le projet et convaincue de ses avantages, il pourrait y avoir des soucis de disponibilité des ressources humaines nécessaires.

Il y a aussi des risques additionnels liés au recours à une agence externe de développement logiciel pour créer des services et clients pour UXP.

Il est recommandé de :

- Inclure des développeurs de l'agence externe dans la formation UXP des développeurs ;
- Prévoir un support supplémentaire potentiellement requis par l'INNORPI pour le développement des services et clients.

L'ATTT n'a pas de développeurs de web services expérimentés.

Pendant la réunion avec l'ATTT, il a été déduit que malgré le fait qu'elle ait des développeurs, ces derniers n'ont pas d'expérience dans le développement des web services SOAP. Même si la formation UXP remédie partiellement à ce problème, il est recommandé de :

- Prévoir des formations supplémentaires pour les employés de l'ATTT
- Prévoir un support supplémentaire dans le développement des services et clients pour l'ATTT.

Le service MoF4 doit être approuvé pour être développé.

Le MoF4 est un service demandé par l'INNORPI, la CNSS et la DGD en vue d'obtenir des informations détaillées sur un contribuable à partir de son matricule fiscal. Ce service a pour but de synchroniser les informations entre les organisations quand il y a une mise à jour. Mais vu le périmètre de ce service,

la DGI doit l'approuver avant de le mettre en œuvre.

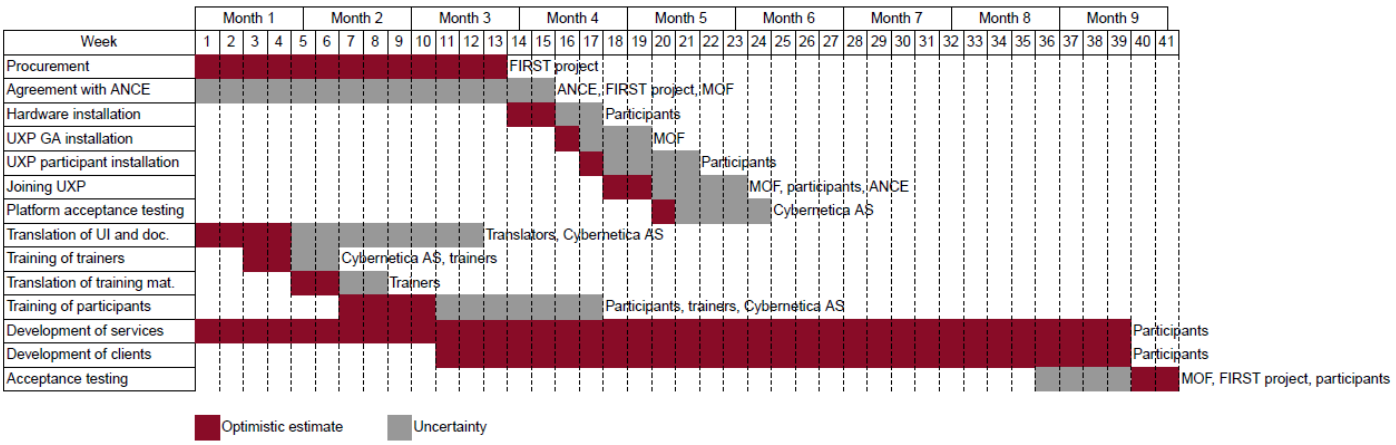
Il est recommandé d'essayer d'obtenir cette approbation le plus tôt possible. Faute d'approbation, le périmètre du service doit être réduit jusqu'à ce qu'une approbation puisse être obtenue.

L'ANSI n'a pas été consultée au sujet de ce projet.

La Tunisie a une agence nationale de sécurité informatique (ANSI). Cette agence ne fait actuellement pas partie du projet et n'a pas été consultée au sujet des enjeux potentiels en découlant. Bien qu'il semblerait que le rôle de l'ANSI soit plutôt consultatif que réglementaire, il est recommandé d'avoir le support de l'ANSI le plutôt possible afin d'éviter tout retard possible pendant les phases plus avancées du projet.

12. Plan du projet

Un aperçu sur le calendrier du projet



Acquisition (Procurement)

Temps estimé : 13 semaines (3 mois). Acteurs : le projet FIRST.

Le but de l'activité d'acquisition est d'obtenir le matériel et les logiciels requis pour que les participants puissent adhérer à la plateforme UXP et mettre en œuvre les services et les clients compris dans le projet. Les étapes suivantes doivent être réalisées :

1. Compiler une liste complète du matériel requis et des licences de logiciels nécessaires en se basant sur ce rapport et des consultations avec les participants. Il faut noter que cette liste doit comprendre tout autre matériel nécessaire mais non spécifié dans ce rapport, en l'occurrence le matériel de montage, les câbles, etc.
2. Sélectionner les fournisseurs.
3. Commander le matériel et les logiciels requis.
4. Distribuer le matériel aux participants selon leur besoin.

L'accord avec la ANCE (Agreement with ANCE)

Temps estimé : n/a. Acteurs : ANCE, le projet FIRST, MoF

Le projet FIRST et le MoF doivent conclure un accord avec l'ANCE qui agira comme l'autorité de certification principale (root CA) de l'environnement de production UXP. Cet accord doit exister avant même de commencer l'installation des composantes UXP. Le MoF doit formuler des directives pour les participants décrivant la manière d'obtenir les certificats requis pour l'utilisation d'UXP de la part de l'ANCE.

L'installation du matériel (Hardware installation)

Temps estimé : 2 semaines. Acteurs : les participants.

Les participants sont tenus d'installer le matériel fourni et distribué par le projet FIRST dans leurs centres des données respectifs. Les informations nécessaires à la configuration des systèmes d'exploitation, du réseau et des pare-feu pour UXP seront fournies aux participants lors de la formation des administrateurs des serveurs de sécurité UXP.

Il faut réaliser les étapes suivantes :

1. Installer les serveurs et les HSMs physiquement dans les centres des données.
2. Dans le cas de serveurs virtuels, créer les machines virtuelles nécessaires.
3. Installer les systèmes d'exploitation sur les serveurs. Le serveur de sécurité UXP nécessite le système d'exploitation Ubuntu Server.
4. Configurer les interfaces réseau et les règles des pare-feu.
5. Connecter les HSM aux serveurs exécutant le serveur de sécurité UXP.

L'installation de l'autorité gouvernante UXP (UXP GA installation)

Temps estimé : 1 semaine. Acteurs : MoF, ANCE.

Le MoF doit élaborer la liste finale des catégories des membres (organisations) et attribuer un code de membre (organisation) unique à chaque organisation participante.
Le MoF doit installer et configurer les composantes UXP, y compris ce qui suit :

- Serveur de registre UXP (nécessaire pour l'activité suivante)
- Serveur de sécurité UXP (nécessaire pour l'activité suivante)
- Autorité de certification (CA) UXP et autorité d'enregistrement (RA) UXP (nécessaires pour l'environnement de test)

L'installation d'UXP chez les participants (UXP participant installation)

Temps estimé : 1 semaine. Acteurs : les participants.
Les participants doivent installer et configurer le logiciel du serveur de sécurité UXP.

Rejoindre UXP (Joining UXP)

Temps estimé : 2 semaines. Acteurs : participants, MoF, ANCE.

Les participants doivent soumettre des Demandes de Signature des Certificats (CSR) à l'ANCE selon les directives du MoF, recevoir et importer les certificats signés de la part de l'ANCE et soumettre ces mêmes certificats au MoF pour l'approbation finale de rejoindre UXP.

Test de l'acceptation de la plateforme (Platform acceptance testing)

Temps estimé : 1 semaine. Acteurs : Cybernetica AS, participants.

Afin d'évaluer si l'installation des composantes UXP a été accomplie correctement et selon les bonnes pratiques recommandées, Cybernetica AS peut évaluer l'installation. Quoiqu'elle ne soit pas strictement nécessaire, une telle évaluation est une garantie de plus de la bonne installation de la plateforme. Il y a deux options pour mener cette évaluation :

- Pour une évaluation à distance, Cybernetica AS aura besoin d'accès remote SSH aux serveurs de sécurité installés.
- Pour une évaluation locale, un représentant de Cybernetica AS a besoin de se déplacer physiquement sur place pour accéder aux serveurs de sécurité installés.

Traduction de l'interface de l'utilisateur et de la documentation (Translation of user interface and documentation)

Temps estimé : 4 semaines. Acteurs : traducteurs, Cybernetica AS.

La documentation et l'interface UXP doivent être traduites en Français ou en Arabe. La Section 10.1 décrit le processus en détail. Cette activité comporte les étapes suivantes :

1. Sélection des traducteurs.
2. Envoi par Cybernetica AS de la documentation et des fichiers de traduction de l'interface en anglais aux traducteurs.
3. Traduction des documents et de l'interface utilisateurs.
4. les documents traduits sont fournis aux formateurs qui ont suivi la formation des formateurs UXP.
5. Les formateurs donnent leur avis sur l'exactitude de la traduction et l'utilisation correcte de la terminologie. Les versions traduites seront révisées par les traducteurs à la lumière des commentaires des formateurs.
6. La traduction et les commentaires sur la traduction des illustrations sont soumis à Cybernetica AS.
7. Cybernetica AS prépare les illustrations traduites, des packages de traduction pour UXP et les versions PDF de la documentation traduite.

Formation des formateurs (Training of trainers)

Temps estimé : 2 semaines. Acteurs : Cybernetica AS, formateurs.

Le but de cette activité est de préparer un groupe de spécialistes capables d'enseigner l'utilisation d'UXP et le développement des web services et de clients déployables sur UXP au personnel des organisations participantes. La Section 8 offre une explication détaillée de la formation.

Traduction du matériel de la formation (Translation of training materials)

Temps estimé : 2 semaines. Acteurs : Formateurs.

Après l'accomplissement de la formation des formateurs, Cybernetica AS fournira les supports de formation en anglais. Il est attendu que les formateurs les traduisent en Français pour les préparer

à la formation subséquente des participants.

Formation des participants (Training of participants)

Temps estimé : 4 semaines. Acteurs : participants, formateurs, Cybernetica AS.

Les formateurs doivent former le personnel des organisations participantes. Cybernetica AS peut fournir son support pendant la formation en cas de questions complexes.

Développement des services (Development of services)

Temps estimé : 39 semaines (8.5 mois). Acteurs : participants.

Les participants doivent concevoir et implémenter des web services qui seront déployés sur UXP. Pendant cette phase, le MoF doit clairement expliquer aux participants les services que le MoF va consommer, leurs données en entrées, les résultats attendus en sortie et l'utilité de ces résultats pour le MoF. Le MoF doit collaborer avec chaque organisation participante et donner son avis relatif à chaque service *pendant* son développement.

Le MoF doit aussi développer ses propres services et solliciter l'avis des participants consommateurs de ces services *pendant* leur développement.

Développement des clients (Development of clients)

Temps estimé : 29 semaines (6 mois). Acteurs : participants.

Les participants doivent concevoir et mettre en œuvre des clients pour consommer les services déployés sur UXP. Les clients doivent donner leur avis sur les services et les fournisseurs de services doivent être prêts à modifier les services si nécessaire.

Tests d'acceptation (Acceptance testing)

Temps estimé : 2 semaines (0,5 mois). Acteurs : MoF, participants.

Le but de cette phase est d'évaluer si les objectifs du projet pilote ont été atteints. Pour chaque cas d'usage, il faut au moins considérer ces points :

1. Est-ce que le fournisseur de service a bel et bien créé et développé le service nécessaire ?
2. Le service était-il déployé dans l'environnement de test avec des données de test ?
3. Est-ce que les autres participants concernés ont reçu la description du service par le fournisseur du service ?
4. Est-ce que la documentation sur le service est suffisante et correcte ?
5. Est-ce que le logiciel client a été implémenté par les consommateurs prévus ?
6. L'implémentation du logiciel client respecte-t-elle la documentation que le fournisseur du service a fournie ?
7. Est-ce que le client est connecté à UXP ?
8. Est-ce que le client est capable d'utiliser le service ?
9. Y-a-t-il eu suffisamment de test du service et du client de la part des parties concernées ?
10. Est-ce que le service et le client ont été déployés dans l'environnement de production après le

test ?

11. Est-ce que le client reçoit des informations exactes du service dans l'environnement de production ?
12. Est-ce que les informations reçues par le client sont en fait exploitées ?
13. Le service a-t-il rempli les objectifs prévus ?

12.1. Développement des services et des clients

Les services déployés sur UXP et les clients consommant ces services doivent être développés par les organisations participantes. Chaque organisation participante doit gérer son projet de développement logiciel. Elle doit aussi coordonner le développement des services avec les participants qui les consommeront et le développement des clients avec les fournisseurs de service.

Les cas d'usage sélectionnés pour le pilote n'incluent que ceux qui mettent en œuvre un échange de données entre un participant et le MoF. Quoique l'échange de données entre d'autres participants puisse se faire à travers la même plateforme, il ne fait pas partie du périmètre de ce projet pilote. En raison de cette décision, les participants ne sont tenus de coordonner le développement qu'avec le MoF.

Les services à déployer sur UXP peuvent être développés en parallèle à l'installation de la plateforme en suivant les spécifications du UXP Message Protocol. Cette section indique quelques critères de base pour les services et les clients utilisant UXP. Les détails seront expliqués pendant les sessions de formation des développeurs.

Critères de base pour un service SOAP compatible avec UXP

1. Le service doit utiliser SOAP 1.1 ou SOAP 1.2 en utilisant la sérialisation XML 1.0. Le transport HTTP est utilisé pour les deux versions de SOAP.
2. Il doit y avoir une description WSDL valide du service. Si des schémas XML externes sont utilisés, ces schémas doivent être publiquement disponibles ou directement incorporés dans le document WSDL.
3. Chaque service UXP correspond à une seule *opération* définie en utilisant WSDL.

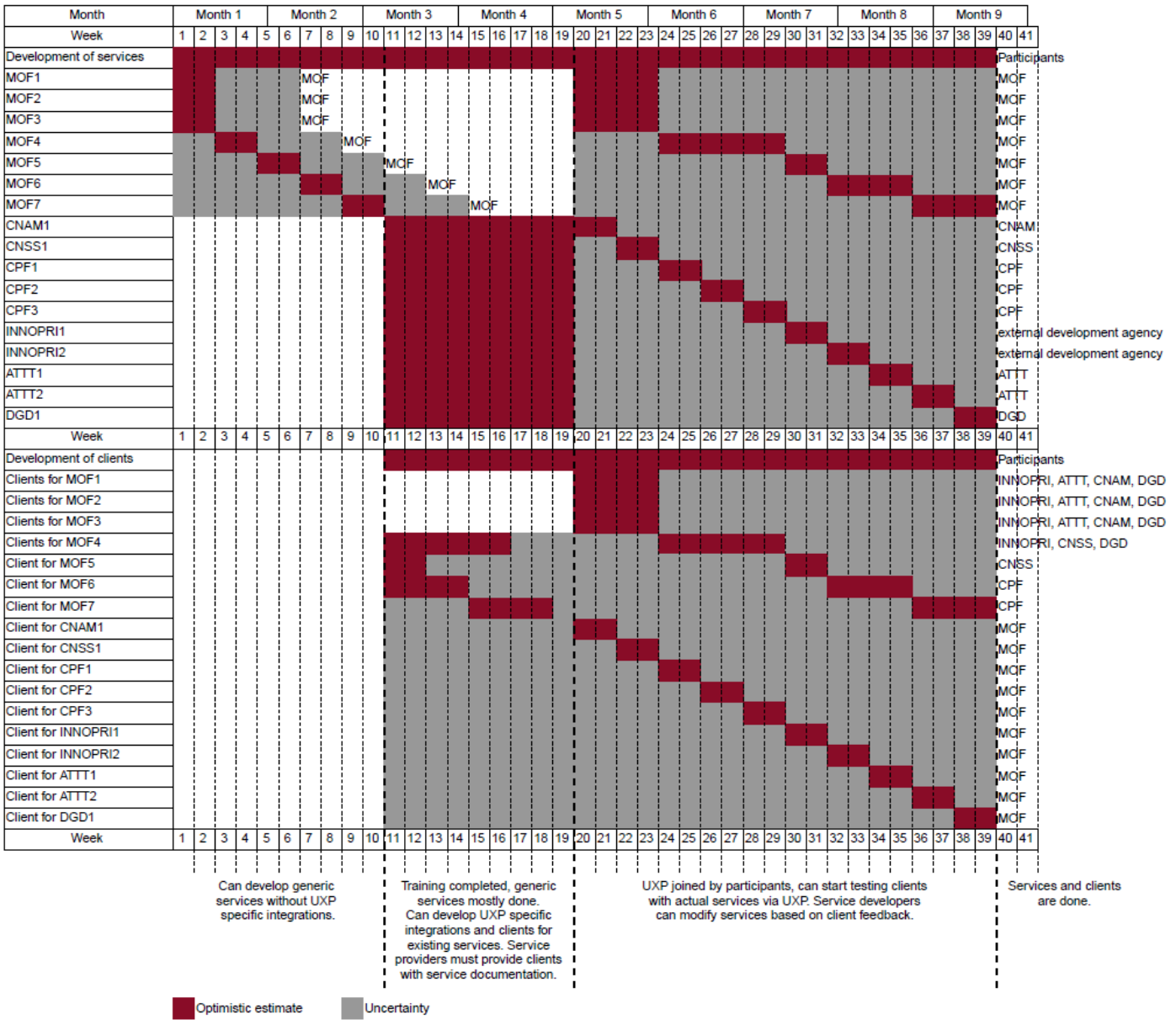
Afin de développer un client pour un service, l'organisation développant le client a besoin d'obtenir la documentation du service, y compris la description WSDL du service, de la part du fournisseur du service. Ceci peut se faire même avant l'installation d'UXP, mais les spécifications du service doivent être raisonnablement proches de leurs versions finales. Le client peut alors être développé en utilisant un service fictif. Il sera tout de même impossible de tester le client avec le service réel avant qu'UXP ne soit complètement installé et que les participants soient connectés à la plateforme.

Critères de base pour un client d'un service SOAP déployé via UXP

1. Le client doit être conforme à la spécification du service. Les messages que le client génère doivent être valables selon la description WSDL du service.
2. Le client doit ajouter à ses demandes des en-têtes SOAP spécifiques à UXP avant de les envoyer au serveur de sécurité UXP.
3. Le client doit être capable de traiter les erreurs SOAP possibles. Il y a des erreurs SOAP qui peuvent être générées par le serveur de sécurité UXP en cas de soucis de connectivité ou de configuration d'UXP.

Quand toutes les composantes UXP sont installées et que les participants ont adhéré à UXP, l'environnement de test d'UXP peut être utilisé pour tester des clients avec des services réels. Notez que les services et les clients ne doivent jamais envoyer des données réelles dans l'environnement de test.
Pendant ces tests, les clients peuvent découvrir des incompatibilités entre les clients et les services réels. Les fournisseurs des services et les clients qui les consomment doivent collaborer pour pouvoir résoudre de telles incompatibilités.
Toute incompatibilité doit être traitée et résolue avant que les clients et les services ne soient déployés dans l'environnement de production avec les données réelles.

Une répartition possible dans le calendrier du développement des services et des clients :



Le calendrier, ci-dessus, montre un exemple de répartition possible sur l'axe temps des développements des clients et services prévus pour tous les participants. Il est important de noter que ce calendrier n'est qu'un exemple. Les principes directeurs de planification du développement des services et des clients

sont les suivants :

- Les web services doivent être conçus et développés avant que les clients consommant ces services ne puissent être implémentés.
- Pendant les tests d'intégration entre clients et services réels, des incompatibilités peuvent être révélées. La modification d'un service et de tous les clients consommant ce service peut être nécessaire pour traiter ces incompatibilités d'une manière satisfaisante. Si c'est faisable, il est préférable d'opter pour la modification de clients individuels.
- Les tests d'intégration entre clients et services réels ne peut commencer que lorsque toutes les composantes UXP sont installées et que les participants ont rejoint la plateforme.