Point 05
Téléphonie Mobile Sécurisée Interministérielle et Messagerie Instantanée de l'Etat

1. CONTEXTE ET ENJEUX

Les risques liés aux outils de communication professionnels concernent particulièrement les centres de décision de l'Etat, et une circulaire du Premier ministre du 25 mars 2015 demandait à ce que les cabinets ministériels mettent en œuvre les moyens adéquats pour **protéger leur messagerie et leurs échanges par voix et SMS**.

Une **solution technique commune,** (les téléphones mobiles sécurisés ERCOM « CryptoSmart ») a été retenue en 2016 dans l'objectif de sécuriser les terminaux et les communications des cabinets ministériels. Certains ministères disposaient déjà de cette solution (Ministère des Armées, Affaires étrangères, Finances, Intérieur, ainsi que les services du Premier ministre et la Présidence) alors que d'autres étaient encore à équiper.

Compte tenu du coût d'entrée de cette solution (plus de 600 k€ pour chaque entité), le déploiement d'une **plateforme interministérielle** a été réalisé en 2017 pour permettre le lancement d'un service pour les ministères qui n'étaient pas déjà équipés (Justice, Environnement, Affaires sociales, Agriculture, Education nationale, Culture), avec une infrastructure hébergée par le Ministère des Armées, la fourniture d'équipements et les prestations d'exploitation pour 500 utilisateurs.

Suite à l'équipement des cabinets ministériels en mai 2017, un premier retour d'expérience a montré que les usages évoluent de l'utilisation de la voix et des SMS vers des messageries instantanées (WhatsApp, Telegram…). Pour éviter que les utilisateurs soient tentés de repasser sur des **terminaux et applications non contrôlés** (ce que des mesures d'accompagnement et d'éducation à la sécurité ne permettent pas d'éviter, et ce qui crée des risques de confidentialité des données), il est nécessaire :

- d'une part d'améliorer les fonctions de communication sécurisées des téléphones sécurisés
- d'autre part d'y ajouter une solution de messagerie instantanée maîtrisée

2. MISE EN PLACE DE LA SOLUTION DE MESSAGERIE INSTANTANEE (NOM PROVISOIRE « TCHAP »)

La DINSIC, avec la contribution de l'ANSSI, du ministère des affaires étrangère et du ministère des armées, a entrepris le **développement d'un service de messagerie instantanée de l'Etat**, fournissant des fonctionnalités de messagerie texte et multimédia, en point-à-point et en groupe, des services voix/vidéo, et un annuaire des utilisateurs de l'administration, avec une ergonomie et une qualité de service selon l'état de l'art. Il est développé à partir d'un projet logiciel open-source Riot-Matrix, adapté aux besoins de l'Etat et hébergé par l'administration.

Pour assurer son adoption par le personnel de l'Etat et développer une communauté d'usage, il sera utilisable sur tout type de terminaux mobile (Android et iPhone) et sur ordinateur, au sein des administrations et avec les interlocuteurs externes. Il sera **déployé prioritairement sur les terminaux sécurisés ERCOM**.

Le développement se fait avec plusieurs versions, étendant progressivement les fonctionnalités couvertes. Le périmètre des utilisateurs auprès de qui l'application est fournie pour test/utilisation est aussi progressivement étendu au fil des versions (voir annexe)

La cible visée est une version qui puisse commencer à être déployée dans les cabinets pour le 13 juillet. Cela suppose dans chaque ministère :

- la préparation de la conduite du changement et du support vis-à-vis de son cabinet;
- **l'ajout de Tchap dans les magasins applicatifs des TMSI avant le 6 juillet**.

Le financement des réalisations logicielles et de la maintenance associée est porté en 2018 par la DINSIC, en 2019 un partage des coûts sera mis en place.

S'agissant de l'**hébergement** (actuellement réalisé sur le Cloud externe de l'Etat) le principe à la cible est que chaque ministère héberge et gère sa propre instance. Il est toutefois souhaitable d'envisager que plusieurs ministères s'associent pour mutualiser ces charges. La DINSIC animera la recherche d'une solution dans ce sens au second semestre 2018.

3. PERENNISATION ET DEVELOPPEMENT DE LA SOLUTION DE TELEPHONIE SECURISEE (TMSI)

Aujourd'hui :

- Certains ministères disposent d'une infrastructure ERCOM Cryptosmart et gèrent leur propre parc de terminaux.
- Les autres ministères sont rattachés à l'infrastructure interministérielle ERCOM

En parallèle, la DINSIC coordonne avec les DSI ministérielles des actions d'accompagnement et d'optimisation pour l'utilisation de l'application ERCOM « voix/SMS sécurisés ». Les évolutions demandées à l'industriel ont été livrées, la mise en œuvre relevant des ministères est en cours. La consolidation et la gestion d'un annuaire interministériel reste un point de blocage de certains ministères.

S'agissant des ministères rattachés à l'infrastructure interministérielle ERCOM :

- Jusqu'à fin octobre 2018 : ils bénéficient par convention du financement des infrastructures techniques, de 500 terminaux et de l'exploitation du service.
- A partir du 1er novembre 2018 :
    - Les ministères doivent **mettre en place un marché subséquent à l'accord cadre interministériel** qui sera notifié par le ministère des Armées (DIRISI) en juin 2018, afin de commander des terminaux et prestations spécifiques
    - **Le financement des coûts partagés d'exploitation de l'infrastructure interministérielle de téléphonie mobile sécurisée ERCOM (estimées à 75 k€ mensuel) sera partagé entre ministères** au prorata du nombre de terminaux déjà déployés ; une nouvelle convention multipartite sera rédigée en ce sens.
    - Pour la période initiale de novembre 2018 à février 2019 inclus, ce cofinancement se fera par refacturation, la DINSIC assurant l'avance de trésorerie. Il se fera ensuite par transfert annuel de crédits.

Chaque ministère continue à conforter l'utilisation du téléphone sécurisé par les hautes autorités. Cela passe notamment par :

- assurer que la messagerie électronique n'est pas accessible par des terminaux non sécurisés ;
- déployer Tchap dès que possible sur les terminaux.

A ce titre, il conviendra de rappeler que Tchap lève un frein à l'adoption des TMSI, et que par ailleurs utiliser Tchap sur un autre terminal qu'un terminal sécurisé TMSI ne donne pas le même niveau de garantie de confidentialité que l'utilisation de Tchap sur un terminal non maîtrisé. **La disponibilité de Tchap ne saurait donc être un prétexte pour ne pas utiliser les terminaux TMSI, mais il s'agit au contraire d'un facilitateur.**

PROPOSITIONS SOUMISES A L'AVIS DU CSIC

Validation des actions présentées dans la présente fiche.

4. ANNEXE : FEUILLE DE ROUTE PRODUIT DE TCHAP

Versions	Expérimentations	Preview	V1	V2	V3
Usage	DSI de l'administration	Directeurs d'administration centrale et membres de cabinet	Administrations	Administrations et invités	Grand public et partenaires
Calendrier	cpts temporaires (alpha) en cours cpts pérennes (beta) : 15/6/18	13/7/18	admin. centrales : début sept. autres admin : déploiement sur 2 mois	début novembre 2018	N/D

Accès	Application Android		+ navigateur Web	+ Application iOS	
Distribution de l'application mobile	téléchargement et mise à jour manuelles	**Store privé ERCOM**	Store public		
Inscription	par autoenrôlement des agents avec adresse mail		**+ invitation VIP par adresse mail (exclusivité ERCOM)**	+ enrôlements d'externes sur invitation par adresse mail,	+ autoenrôlement des externes par mail ou n° mobile

Interface utililisateur	Android avec Ux de discussion Riot	Ux Tchap Android (design & expérience)	+ web avec Ux de discussion Riot	+ Ux unifiée	
Types d'échanges	discussions personnelles, salons privés, salons public (ref : whats'app / telegram)			Distinction agent-externe	espaces de travail communautaires (ref : Slack)
Contacts	Synchronisation des contacts locaux avec l'annuaire Tchap				
Identification	Entité d'appartenance suggérée	Appartenance à un domaine (Modernisation, Intérieur, Dév-durable,…)			+ Identité FranceConnect des externes

Infrastructure serveurs (Cloud)	phase alpha : comptes temporaires (1 serveur) phase beta : comptes pérennes administrations centrales (13 serv. en HA)		+ autres serveurs "*.gouv.fr" (env. 25?) + 1 serveur externe (invités VIP)	ouverture de l'instance(s) externe(s)	+ interop. Citadel?
Sécurité	N/A	chiffrement bout-en-bout + Antivirus			

Fonctions expérimentales (support limité)	accès web, accès IoS avec Riot	accès IoS avec Riot	