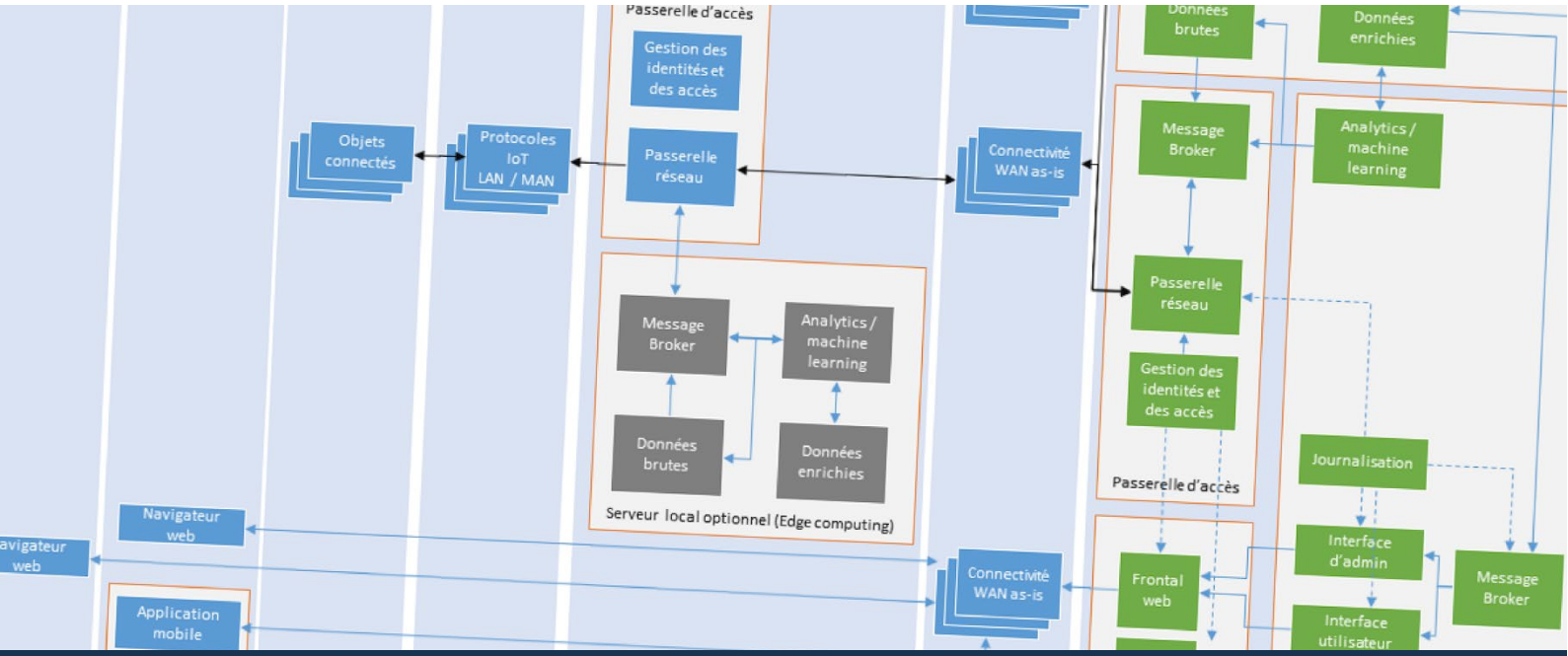
LES FICHES PRATIQUES du CLUSIF - IoT



Quels sont les critères de sécurité pour la sélection des opérateurs, des plateformes et des technologies ?

Version 1.0

1. POURQUOI UNE CONCEPTION SÉCURISÉE

Les projets impliquant des objets connectés nécessitent, du fait de la multiplicité et l'hétérogénéité des éléments matériels interconnectés sur plusieurs couches logicielles, de faire les bons choix des technologies le plus en amont des projets. Il est primordial de choisir les technologies et les opérateurs présentant, dès la conception et par défaut, un niveau de risque de la sécurité de l'information le plus faible possible et adapté à l'usage prévu et aux objectifs de sécurité. Ce constat est valable pour les personnes en charge des activités de conception, de développement, d'intégration et de déploiement, ainsi que pour les utilisateurs des objets connectés.

Quand le socle de sécurité est pensé dès la conception et/ou intégré au produit final sans nécessité de superposer des couches de sécurité conséquentes supplémentaires, l'effort global pour le traitement des risques est réduit et se résume à ajouter quelques mesures de sécurité spécifiques définies à l'issue d'une appréciation des risques. L'enjeu de la sélection avancée des protocoles et des technologies étant la minimisation de cet effort global et la maximisation du niveau initial de sécurité. Ceci est également obligatoire afin de répondre à des exigences légales dépendant de la région où les objets connectés sont commercialisés, comme par exemple la loi californienne sur les objets connectés (Bill Text, SB-327 Information privacy: connected devices) - votée en 2018, qui rentrera en vigueur en 2020 qui stipule que :

- Les mots de passe préprogrammés doivent être uniques à chaque objet connecté manufacturé
- L'objet connecté doit contenir des fonctionnalités qui exigent la modification des moyens d'authentification avant de garantir l'accès et permettre son utilisation pour la première fois

Le niveau global de sécurité est plus élevé quand des mesures de sécurité sont implémentées nativement sur plusieurs couches du système en question, cette implémentation multicouche permet de répondre au principe de défense en profondeur. Il ne faut néanmoins pas se reposer entièrement sur ces mesures du socle de base, car même si les spécifications évoluent sans cesse pour répondre aux nouvelles attaques, une analyse des risques et des mesures complémentaires resteront nécessaires.

gestion des risques de la sécurité de l'information dans les systèmes impliquant les objets connectés. Les fonctions de communication bas-niveau (lien physique -radio-, bande de base, couche liaison) sont assurées en *Bluetooth* par le *Controller* ; les autres fonctions (applicatives, services, etc.) sont effectuées par le « *Host* », une interface *Host Controller Interface* assurant la liaison, avec parfois une implémentation sur le même microprocesseur de ces deux fonctions. Dans cette technologie les transactions se font via une "clé de lien" (*link key*), un nombre aléatoire de 128 bits qui est utilisé lors du processus d'authentification et de chiffrement avec 3 modes de sécurité :

- 1er mode : aucune fonction de sécurité n'est activée,
- 2ème mode (élémentaire) : ce mode implémente une sécurité sur la couche Application après l'établissement d'une liaison,
- 3ème mode (avancé) : il hérite des fonctionnalités du Mode 2 et ajoute une sécurité au niveau de la couche liaison : authentification et chiffrement en amont de la connexion.

2. CRITERES D'EVALUATION

Nous proposons, pour faire un choix, de réaliser une évaluation basée sur un tableau d'aide à la décision et une méthode de notation basée sur des facteurs et des critères pondérés en fonction des besoins de sécurité.
Ces critères doivent porter sur le système connecté ainsi que sur son écosystème :

- Les objets connectés déployés,
- Les protocoles IOT,
- Les interfaces d'accès web, les applications mobiles et les passerelles d'accès,
- Les applications backoffice hébergées sur une infrastructure Cloud,
- La globalité du système voire l'écosystème.

La prise en compte des besoins de sécurité traditionnels (confidentialité, intégrité, disponibilité et traçabilité) ne doit pas être la seule ni la première grille d'analyse des objets connectés. Il faut avoir conscience que les choix des opérateurs et des technologies IoT à utiliser doivent dépendre des exigences fonctionnelles, économiques et techniques exprimées par le métier en priorité.

Le risque doit être évalué en fonction de l'impact sur les métiers ou les données personnelles en cas de compromission des mesures de sécurité.

Dans cette fiche technique nous proposons de construire une liste spécifique de critères prédéterminés à considérer pour le choix des opérateurs et des technologies. Cette liste servira comme un catalogue de critères dont il faut tenir compte en partie ou entièrement en fonction su système étudié, pour gérer la sécurité de l'IOT. Ils viendront compléter ceux habituellement considérés par les utilisateurs à savoir l'ergonomie et l'autonomie ou ceux habituellement considérés par les concepteurs et les développeurs des objets connectés à savoir, le débit, la bande passante, la portée, etc.

nécessiterait un déploiement sur plusieurs éléments constitutifs du système.
Afin d'évaluer les risques de la sécurité de l'information dans le domaine des objets connectés, une liste de critères communs et prédéterminés doit être définie, cette liste permettrait d'effectuer un choix cohérent et rationnel entre les différents opérateurs et technologies. Ces critères doivent permettre de refléter :

- Les sources des menaces et les vecteurs d'attaques,
- Les vulnérabilités et leurs conséquences si elles sont exploitées,
- L'absence de mesures de sécurité adéquates,
- L'efficacité des mesures de sécurité.

Critères	Description
Support Évolutions Pérennité de la plateforme	Taille des éditeurs Âge actuel de la solution et nombre de versions Maturité de la technologie Feuille de route de la solution Présence et vitalité de la communauté d'utilisateurs Réputation des éditeurs sur le support de leurs solutions Origine des plateformes (éditeurs consolidés, sous-traitants, etc.) Contrat / conditions générales d'utilisation
Niveau de certification	De l'objet lui-même De la plateforme
Inscription/Enregistrement ("enrôlement")	Capacité à gérer un jeton authentifiant unique par cible Facilité de mise en service à distance Mécanisme de scellement
Gestion de configuration Profil de sécurité	Définition et affectation de profils d'objet Capacité de mise à jour des profils définis Gestion du cycle de vie de bout en bout
Administration de la solution	Mécanismes d'authentification Profils / privilèges disponibles ou définissables (accès supervision, maintenance, administrateurs, etc.) Authentification des objets Authentification du réseau Authentification de l'utilisateur/abonné
Supervision du parc d'objets	Partage d'information sur les objets déployés Capacité à définir des alertes (ex : autonomie restante, dernier signe de vie, comportement déviant…) Capacité à fournir des journaux Capacité à générer des rapports sur ces mêmes critères Information sur la configuration et l'état
Mise à jour du parc d'objets	Capacité à effectuer des mises à jour Mode "push" et mode "pull" pour les mises à jour Faculté de suivre la version des objets
Gestion des alertes et des aberrations	Capacité à créer et transmettre des alertes Capacité à prendre en compte des écarts extrêmes Faculté d'absorber les faux-positifs (résilience aux Faux ?) Traitement de l'incident
Compatibilité, Interopérabilité	Transparence de l'implémentation OS supportés, couches logicielles utilisées, protocoles implémentés Implémentation mature du réseau

ⓘ Point de vue du RSSI

L'ensemble des critères proposés peuvent servir de base pour construire une politique de sécurité IoT adaptée à l'entreprise ou au cas d'usage considéré.

Il convient de déterminer en amont, lors de la conception de l'objet et de son écosystème, les mesures de sécurité et les critères de choix prépondérants parmi ceux proposés, et en complément de critères fonctionnels et économiques.