Online Trust Alliance
an Internet Society initiative

Cadre de confiance de sécurité et de confidentialité de IoT v2.5

Le cadre de confiance IoT (IoT Trust Framework®) inclut un ensemble de principes stratégiques nécessaires pour sécuriser les terminaux IOT et leurs données lors de leur expédition et tout au long de leur cycle de vie. Grâce à un processus multipartite axé sur le consensus, des critères ont été identifiés pour la maison connectée, le bureau et les technologies portables connectées, y compris les jouets, les trackers d'activité et les appareils de fitness. Le cadre décrit le besoin de divulgations complètes qui doivent être fournies avant l'achat du produit, les politiques concernant la collecte, l'utilisation et le partage des données, ainsi que les modalités et conditions des correctifs de sécurité après la garantie. Les mises à jour de sécurité sont essentielles pour optimiser la protection des appareils IoT lorsque des vulnérabilités sont découvertes et que les attaques évoluent. En outre, le cadre fournit des recommandations aux fabricants pour améliorer la transparence et la communication concernant la capacité des dispositifs à mettre à jour et une série de problèmes liés à la confidentialité des données.

L'application des principes à l'ensemble de la solution ou de l'écosystème de l'appareil est essentielle pour aborder les risques inhérents à la sécurité et les problèmes de confidentialité. Ceux-ci incluent l'appareil ou le capteur, les applications de support et les services backend / cloud. Étant donné que de nombreux produits mis sur le marché reposent sur des composants et logiciels tiers ou open source, il incombe aux développeurs d'appliquer ces principes et de mener des évaluations de la sécurité de la chaîne d'approvisionnement et des risques de confidentialité.

Servant de guide d'évaluation des risques pour les développeurs, les acheteurs et les détaillants, le cadre constitue la base de futurs programmes de certification IoT. L'objectif de l'OTA est de mettre en évidence les appareils qui répondent à ces normes afin d'aider les consommateurs, ainsi que les secteurs publics et privés, à prendre des décisions d'achat informées. Le cadre et les ressources associés sont disponibles sur https://otalliance.org/IoT.

Le cadre est divisé en quatre axes prioritaires :

- **Principes de sécurité** (1-12) - Applicable à n'importe quel appareil ou capteur et à toutes les applications et services de cloud backend. Cela va de l'application d'un processus rigoureux de sécurité de développement logiciel à l'adhésion aux principes de sécurité des données stockées et transmises par l'appareil, à la gestion de la chaîne logistique, aux tests de pénétration et aux programmes de signalement de vulnérabilité. D'autres principes soulignent l'exigence de correctifs de sécurité pour le cycle de vie.
- **Accès utilisateur et informations d'identification** (1-17) - Exigence de cryptage de tous les mots de passe et noms d'utilisateur, envoi d'appareils avec des mots de passe uniques, implémentation de processus de réinitialisation de mot de passe généralement acceptés et intégration de mécanismes pour prévenir les tentatives de connexion par « force brute ».
- **Confidentialité, divulgations et transparence** (18-33) - Exigences conformes aux principes de confidentialité généralement acceptés, y compris les divulgations importantes sur l'emballage, les points de vente et / ou mises en ligne, capacité pour les utilisateurs de réinitialiser les appareils aux paramètres d'usine et conformité aux exigences réglementaires applicables incluant l'EU GDPR et la

réglementation de confidentialité des enfants. Traite également des divulgations sur l'impact des caractéristiques ou fonctionnalités du produit si la connectivité et désactivée.

- **Notifications et bonnes pratiques associées** (34-40) - La clé du maintien de la sécurité des appareils est d'avoir des mécanismes et des processus pour informer rapidement un utilisateur des menaces et des actions requises. Les principes incluent l'authentification par courrier électronique pour les notifications de sécurité et que les messages doivent être communiqués clairement aux utilisateurs de tous les niveaux de lecture. De plus, les exigences d'emballage inviolable et d'accessibilité sont mises en évidence.

OTA IoT Trust Framework® v2.5 – mise à jour 14/10/17

Axé sur les appareils et services de « consommation » pour la maison et l'entreprise, y compris les technologies portables

Cadre de confiance IoT ● Obligatoire (Doit) O Recommandé (Devrait)	
Sécurité - Appareil, applications et services cloud	
1. Indiquer si l'appareil est capable de recevoir des mises à jour liées à la sécurité et, dans l'affirmative, indiquer si l'appareil peut recevoir automatiquement les mises à jour de sécurité et quelle action est requise pour assurer que l'appareil soit correctement mis à jour dans un délai raisonnable.	●
2. S'assurer que les appareils et les applications associées prennent en charge le protocole de sécurité et de cryptographie généralement reconnus, ainsi que les meilleures pratiques. Toutes les données personnellement identifiables en transit et stockées doivent être cryptées en utilisant les normes de sécurité généralement acceptées. Cela inclut mais n'est pas limité aux connexions câblées, Wi-Fi et Bluetooth.	●
3. Tous les sites Web de support IoT doivent entièrement chiffrer la session de l'utilisateur de l'appareil aux services backend. Les meilleures pratiques actuelles incluent HTTPS et HTTP Strict Transport Security (HSTS) par défaut, également appelé AOSSL ou Always On SSL. Les périphériques doivent inclure des mécanismes permettant d'authentifier de manière fiable leurs services backend et leurs applications de supports.[1]	●
4. Les sites de supports IoT doivent mettre en place une surveillance régulière et une amélioration continue de la sécurité du site et des configurations de serveur afin de réduire de manière acceptable l'impact des vulnérabilités. Effectuer des tests de pénétration au moins deux fois par an.[2]	●
5. Établir une divulgation coordonnée des vulnérabilités, y compris des processus et des systèmes pour recevoir, suivre et répondre rapidement aux rapports de vulnérabilité externes de tierces parties, y compris mais sans s'y limiter, les clients, les consommateurs, les universités et la communauté de recherche. Corriger les vulnérabilités et les menaces liées à la conception de versions de produits de manière publiquement responsable, que ce soit par le biais de mises à jour à distance et / ou de notifications de consommateurs exploitables ou d'autres mécanismes efficaces. Les développeurs devraient envisager des programmes de « bug bounty » et des méthodes de crowdsourcing pour aider à identifier les vulnérabilités.	●
6. S'assurer qu'un mécanisme est en place pour des méthodes sécurisées automatisées permettant de fournir des mises à jour de logiciels et / ou de micrologiciels, des correctifs et des révisions. De telles mises à jour doivent être signées et / ou vérifiées comme provenant d'une source fiable, y compris, mais sans y limiter, la signature et la vérification de l'intégrité.	●
7. Les mises à jour et les correctifs ne doivent pas modifier les préférences, la sécurité et / ou les paramètres de confidentialité configurés par l'utilisateur sans la notification de l'utilisateur. Dans le cas où le micrologiciel ou le logiciel de l'appareil est placé, lors de la première utilisation, l'utilisateur doit avoir la possibilité d'examiner et de sélectionner les paramètres de confidentialité.	●
8. Le processus de mise à jour de sécurité doit indiquer s'il est automatisé (par rapport à automatique). Les mises à jour automatisées permettent aux utilisateurs d'approuver, d'autoriser ou de rejeter les mises à jour. Dans certain cas, l'utilisateur peut vouloir décider comment et quand les mises à jour sont faites, y compris, mais sans y limiter, la consommation de données et la connexion via leur opérateur mobile ou leur connexion ISP. Inversement, les mises à jour automatiques sont transmises à l'appareil de manière transparente sans interaction de l'utilisateur et peuvent ou non fournir des avis à l'utilisateur.	●

9. S'assurer que tous les appareils IoT et les logiciels associés ont été soumis à des tests de cycle de vie rigoureux et standardisés incluant des tests d'unité, de système, d'acceptation et de régression et de modélisation des menaces, ainsi qu'un inventaire de la source pour tout code tiers / open source et / ou composants. Utiliser des techniques de renforcement du code et du système généralement acceptées dans une gamme de scénarios d'utilisation types, y compris la prévention des fuites de données entre l'appareil, les applications et les services cloud. Pour développer un logiciel sécurisé, il faut penser à la sécurité depuis la création d'un projet jusqu'à la mise en œuvre, le test et le déploiement. Les périphériques doivent être livrés avec le logiciel actuel et / ou avec des mises à jour automatiques au premier démarrage pour résoudre les vulnérabilités critiques connues.	●
10. Effectuer des évaluations des risques de sécurité et de conformité pour tous les fournisseurs de services et de cloud. Voir le guide de ressources IoT https://otalliance.org/IoT	●
11. Développer et maintenir une « nomenclature » comprenant des logiciels, des microprogrammes, du matériel et des bibliothèques de logiciels tiers (y compris des modules open source et des plug-ins). Cela s'applique aux périphériques, aux services mobiles et au cloud pour aider à corriger rapidement les vulnérabilités signalées.	◘
12. Concevoir des dispositifs aux exigences minimales nécessaires pour l'opération. Par exemple, les ports USB ou les logements de carte mémoire ne doivent être inclus que s'ils sont nécessaires au fonctionnement et à la maintenance de l'appareil. Les ports et services inutilisés doivent être désactivés.	●
Accès utilisateur et informations d'identification	
13. Inclure l'authentification forte par défaut, y compris la fourniture de mots de passe uniques, générés par le système ou à usage unique ; ou bien utiliser des informations d'identification de certificat sécurisées. Au besoin, exiger l'utilisation de mots de passe uniques pour l'accès administratif, la délimitation entre les appareils et les services et l'impact respectif des réinitialisations d'usine.	●
14. Fournir des mécanismes de récupération généralement acceptés pour les applications IoT et prendre en charge les mots de passe et / ou les mécanismes de réinitialisation des informations d'identification à l'aide de la vérification et de l'authentification multifactorielle (courriel et téléphone, etc.) là ou aucun mot de passe utilisateur n'existe.	●
15. Prendre des mesures de protection contre la « force brute » et / ou d'autres tentatives de connexion abusives (telles que les robots de connexion automatisés, etc.) en verrouillant ou en désactivant les comptes utilisateur et périphérique après un nombre raisonnable de tentatives de connexion non valides.	●
16. Fournir aux utilisateurs une notification de réinitialisation ou de modification du mot de passe en utilisant une authentification sécurisée et / ou des notifications hors bande.	●
17. Les informations d'authentification, y compris, mais sans y limiter, les mots de passe des utilisateurs doivent être salés, hachés et / ou cryptés. S'applique à toutes les informations d'identification stockées pour empêcher les accès non autorisés et les attaques par force brute.	●
Confidentialité, divulgations et transparence	
18. Veiller à ce que les règles de confidentialité, de sécurité et de support soient facilement identifiables, claires et facilement accessibles avant l'achat, l'activation, le téléchargement ou l'inscription. En plus du placement bien visible sur l'emballage du produit et sur leur site Web, il est recommandé aux entreprises d'utiliser des codes QR, des URL courtes conviviales et d'autres méthodes similaires dans les points de vente.	●
19. Divulguer la durée et la sécurité en fin de vie ainsi que la prise en charge des correctifs (au-delà de la garantie du produit). L'assistance peut prendre fin à une date d'expiration, par exemple le 1er janvier 2025, ou pour une durée spécifique à compter de la date d'achat,	●

non contrairement à une garantie traditionnelle. Idéalement, ces divulgations devraient être alignées sur la durée de vie prévue de l'appareil et communiquées au consommateur avant l'achat. *(Il est reconnu que les périphériques IoT ne peuvent pas être indéfiniment sécurisés et facilement accessibles. Envisager de communiquer les risques liés à l'utilisation d'un périphérique au-delà de sa date d'utilisation, ainsi que l'impact et les risques pour les autres si les avertissements sont ignorés ou si l'appareil n'est pas retiré).* Si les utilisateurs doivent payer des frais ou souscrire un contrat d'assistance annuel, cela doit être indiqué avant l'achat.	
20. Divulguer de manière visible quels types et attributs de données personnelles et identifiables sont collectés et comment ils sont utilisés, en limitant la collecte des données raisonnablement utiles pour la fonctionnalité et l'objectif de la collecte. Divulguer et fournir l'adhésion du consommateur à tout autre fin.	●
21. Divulguer quelles fonctionnalités ne fonctionneront pas si les services de connectivité ou de backend sont désactivés ou arrêtés, y compris, mais sans y limiter, l'impact potentiel sur la sécurité physique. Indiquer ce qui se passe lorsque l'appareil ne reçoit plus les mises à jour de sécurité ou si l'utilisateur ne parvient pas à mettre à jour l'appareil. *(Envisager d'intégrer des contrôles pour désactiver la connectivité ou désactiver les ports afin d'atténuer les menaces potentielles, tout en conservant la fonctionnalité principale du produit, en fonction de l'utilisation du périphérique, en équilibrant les problèmes de vie / sécurité potentiels).*	●
22. Divulguer la politique de conservation de données et la durée de conservation des informations personnelles identifiables.	●
23. Les appareils IoT doivent fournir un avis et / ou demander une confirmation à l'utilisateur lors du couplage, de l'intégration et / ou de la connexion avec d'autres appareils, plateformes ou services.	●
24. Divulguer si et comment la propriété de l'appareil / produit / service IoT et les données peuvent être transférées (par exemple, une maison connectée étant vendue à un nouveau propriétaire ou la vente d'un tracker de fitness).	●
25. Partager les données personnelles des consommateurs avec des tiers uniquement avec le consentement explicite des consommateurs, à moins que cela ne soit requis et limité pour l'utilisation des fonctionnalités du produit ou le fonctionnement du service. Exiger que les fournisseurs de services tiers soient tenus de respecter les mêmes politiques, y compris la conservation de ces données à titre confidentiel et les exigences de notification de tout incident de perte ou de violation de données et / ou d'accès non autorisé.	●
26. Fournir des contrôles et / ou la documentation permettant aux consommateurs d'examiner et de modifier les préférences de confidentialité de l'appareil IoT, y compris la possibilité de réinitialiser au « réglage usine ».	●
27. S'engager à ne pas vendre ou transférer des données de consommation identifiables sauf si elles sont dépendantes de la vente ou de la liquidation de l'activité principale qui a initialement collecté les données, à condition que la politique de confidentialité de l'acquéreur n'en modifie pas les termes. Sinon, un avis et un consentement doivent être obtenus.	●
28. Fournir la possibilité pour un consommateur de retourner un produit sans frais après avoir examiné les pratiques de confidentialité qui sont représentées avant l'opération, à condition que ces termes ne soient pas divulgués de façon visible avant l'achat. Le terme (nombre de jours) pour les retours de produits doit être conforme aux politiques d'échange en vigueur du détaillant, ou spécifié à l'avance.	●
29. Chaque fois que l'opportunité de refuser ou renoncer à une politique est présentée, les conséquences doivent être clairement et objectivement expliquées, y compris tout impacte sur les caractéristiques ou les fonctionnalités du produit. Il est recommandé que la valeur d'adhésion et / ou de partage des données de l'utilisateur soit communiquée à l'utilisateur final.	●
30. Se conformer aux réglementations applicables, y compris, mais sans y limiter, à la Children's Online Privacy Protection Act (COPPA) et aux exigences internationales en matière de confidentialité, de sécurité et de transfert de données.[3] [4]	●
31. Publier publiquement l'historique des modifications apportées à l'avis de confidentialité pour un minimum de deux ans. Les meilleures pratiques comprennent l'horodatage, les redlines et un résumé des impacts des changements.	●

32. Fournir à l'utilisateur ou au mandataire la possibilité de supprimer, ou de rendre anonymes, des données personnelles ou sensibles stockées sur les serveurs de l'entreprise (autre que l'historique de transaction d'achat) en cas d'interruption, de perte ou de vente de l'appareil.	O
33. Fournir la possibilité de réinitialiser un appareil et une application aux paramètres d'usine, y compris la possibilité d'effacer les données de l'utilisateur en cas de transfert, de location, de perte ou de vente.	O
Notifications et bonnes pratiques associées	
34. Les communications de l'utilisateur final, y compris mais sans s'y limiter, les emails et les SMS, doivent adopter des protocoles d'authentification pour aider à prévenir le harponnage et l'usurpation d'identité. Les domaines doivent implémenter SPF, DKIM et DMARC pour toutes les communications et notifications relatives à la sécurité et à la confidentialité, ainsi que pour les domaines parqués et ceux qui n'envoient jamais d'emails.[5]	●
35. Pour les communications par email, dans les 180 jours suivant la publication d'une stratégie DMARC, implémenter une stratégie de rejet ou de mise en quarantaine, qui aide les fournisseurs d'accès et les réseaux récepteurs à rejeter les emails échouant les vérifications d'authentification.[6]	O
36. Les fournisseurs d'IoT utilisant la communication par email devraient adopter la confidentialité au niveau du transport, y compris les techniques de sécurité généralement acceptées pour sécuriser la communication et améliorer la confidentialité et l'intégrité du message (également appelé « TLS opportuniste pour email »).[7]	O
37. Mettre en œuvre des mesures pour aider à prévenir ou à rendre évidente toute altération physique des appareils. Des telles mesures permettent de protéger l'appareil contre l'ouverture ou la modification à des fins malveillantes après l'installation ou d'être renvoyé à un revendeur dans un état compromis.	O
38. Réfléchir à la façon de répondre aux exigences d'accessibilité pour les utilisateurs qui peuvent être malvoyants ou malentendants afin de maximiser l'accès pour les utilisateurs de toutes les capacités physiques.	O
39. Développer des processus de communication pour maximiser la sensibilisation des utilisateurs à tout problème potentiel de sécurité ou de confidentialité, aux notifications de fin de vie et aux rappels de produits éventuels, y compris les notifications dans l'application. Les communications doivent être écrites en maximisant la compréhension pour le niveau de lecture de l'utilisateur général. Envisager des communications multilingues, en reconnaissant que l'anglais peut être la « deuxième langue » pour les utilisateurs (voir les principes connexes concernant la sécurité et l'intégrité des messages).	●
40. Adopter un plan d'intervention et de cyber-réponse et de notification du consommateur à réévaluer, tester et mettre à jour au moins une fois par an et / ou après d'importants changements internes au système, techniques et / ou opérationnels.	●

Les ressources et les mises à jour sont affichées sur https://otalliance.org/IoT

Terminologies, définitions et clarifications

1. Portée - Axé sur les appareils et services de « consommation pour la maison et l'entreprise, y compris les technologies portables ». Les voitures intelligentes, y compris les véhicules autonomes, automoteurs, ainsi que les dispositifs médicaux et les données HIPAA[8] dépassent la portée du cadre, mais la majorité des critères sont jugés applicables. Respectivement, ils relèvent de la surveillance réglementaire de la National Highway Traffic Safety Administration (NHTSA) et la Food and Drug Administration (FDA), [9]
2. Les termes fabricants d'appareils, fournisseurs, développeurs d'applications, fournisseurs de services et opérateurs de plateformes sont tous impliqués par le terme « société ».
3. Il est prévu que les sociétés divulguent des cas de partage de données avec les forces de l'ordre et se réfèrent à tous les rapports de transparence applicables comme légalement autorisés.
4. Les appareils intelligents se réfèrent à des appareils (et des capteurs) qui sont en réseau et ne peuvent avoir que des communications unidirectionnelles.

[1] https://otalliance.org/resources/always-ssl-aossl
[2] https://otalliance.org/blog/responsible-coordinated-ethical-vulnerability-disclosures
[3] Les entreprises, produits et services doivent se conformer à toute loi ou réglementation de la juridiction qui régit la collecte et le traitement des informations personnelles et sensibles, y compris, mais sans s'y limiter, le respect du cadre UE-US Privacy Shield www.commerce.gov/privacyshield et / ou le règlement général de l'UE sur la protection des données (GDPR) www.eugdpr.org. Le non-respect peut constituer un non-respect de ce cadre.
[4] COPPA https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule
[5] Authentification par email - https://otalliance.org/eauth
[6] DMARC -https://otalliance.org/resources/dmarc
[7] TLS for Email - https://otalliance.org/best-practices/transport-layered-security-tls-email
[8] U.S. Ministère américain de la Santé des Services Sociaux, Protection des renseignements personnels sur la santé http://www.hhs.gov/hipaa/index.html
[9] http://www.nhtsa.gov/Vehicle+Safety et http://www.fda.gov/MedicalDevices/default.htm

---

L'OTA est une initiative de l'Internet Society, un organisme de bienfaisance 501c3 à but non lucratif dont la mission est de promouvoir le développement, l'évolution et l'utilisation d'Internet au profit de tous les peuples du monde. La mission de l'OTA est d'améliorer la confiance en ligne, la responsabilisation des utilisateurs et l'innovation en organisant des initiatives multipartites, en développant et en promouvant les meilleures pratiques, les pratiques de confidentialité responsables et la gestion des données. Pour en savoir plus, visitez https://otalliance.org et https://www.internetsociety.org.

R1014