digital.security

« IoT Qualified as Secured »

Labellisation de la sécurité des Solutions IoT

Référentiel des exigences de sécurité

1 janvier 2019

Version du document : 1.0

HISTORIQUE DES EVOLUTIONS

Version	Date	Paragraphe	Action	Nature de l'évolution
1.0	01/01/2019	Tous	Validation	Version finale 1.0
1.1	18/07/2019	PST 4.04	Validation	Correction d'une erreur

SOMMAIRE

1. PREAMBULE

Le programme de labellisation « IQS : IoT Qualified as Secured » (désignation abrégée en « IQS » dans la suite du document) est proposé par digital.security aux acteurs de l'Internet des Objets (IoT) désireux de faire vérifier, par un tiers indépendant, la sécurité de leurs Solutions IoT.

Le Label IQS a pour objet de constituer un indicateur fiable, permettant d'informer avec objectivité les futurs acquéreurs de Solutions IoT, particuliers ou professionnels, sur la sécurité des objets connectés et des services associés disponibles sur le marché.

A cet effet, le Label IQS est délivré par digital.security aux seules Solutions IoT ayant démontré qu'elles satisfont à un ensemble d'exigences de sécurité publiées au sein du présent document, qui constitue le Référentiel des exigences de sécurité du Label « IQS : IoT Qualified as Secured ».

Ces exigences sont établies en regard du niveau de labellisation visé :

- Labellisation de « Niveau Standard » pour laquelle l'évaluation de la Solution IoT porte sur :
  - sa conformité à chacune des exigences de sécurité qualifiées de standard [STD] dans le présent Référentiel et constituant l'état de l'art des mesures de sécurité applicables dans le domaine de l'IoT ;
  - sa conformité, en supplément, à certaines exigences de sécurité posées par d'éventuelles dispositions réglementaires auxquelles est soumise la Solution IoT, spécifiquement identifiées comme telles [REG] dans ce Référentiel.
- Labellisation de « Niveau Avancé » pour laquelle l'évaluation de la Solution IoT porte sur :
  - sa conformité à l'ensemble des exigences spécifiées au « Niveau Standard » ;
  - sa conformité à chacune des exigences de sécurité qualifiées d'avancées [AVC] dans le présent Référentiel, permettant de renforcer la protection de la Solution IoT et de délivrer un niveau de confiance supplémentaire jugé nécessaire par son fournisseur.

2. STRUCTURE DU REFERENTIEL D'EXIGENCES DE SECURITE

THEMES :		EXIGENCES :		
PED.	Protection des échanges de données			
	PED.1. Chiffrement des échanges de données			
		PED.1.01.	Chiffrement des échanges de données sensibles	☑ STD ☐ AVC ☐ REG
		PED.1.02.	Chiffrement de tous les échanges de données	☐ STD ☑ AVC ☐ REG
		PED.1.03.	Robustesse des clés de chiffrement	☑ STD ☐ AVC ☐ REG
	PED.2. Contrôle d'intégrité des échanges			
		PED.2.01.	Contrôle d'intégrité des échanges de données sensibles	☑ STD ☐ AVC ☐ REG
		PED.2.02.	Contrôle d'intégrité de tous les échanges de données	☐ STD ☑ AVC ☐ REG
		PED.2.03.	Authentification mutuelle des échanges de données	☐ STD ☑ AVC ☐ REG
		PED.2.04.	Non rejeu de tous les échanges de données	☑ STD ☐ AVC ☐ REG

PST.	Protection des socles techniques				
	PST.1.	Durcissement des configurations matérielles			
			PST.1.01.	Protection des interfaces de débogage	☑ STD ☐ AVC ☐ REG
	PST.2.	Protection physique des équipements			
			PST.2.01.	Détection d'ouverture du boîtier	☐ STD ☑ AVC ☐ REG
	PST.3.	Durcissement des configurations logicielles			
			PST.3.01.	Prise en compte des vulnérabilités publiées par l'OWASP	☑ STD ☐ AVC ☐ REG
			PST.3.02.	Restriction des services	☑ STD ☐ AVC ☐ REG
	PST.4.	Maintien en conditions de sécurité			
			PST.4.01.	Dispositif de correction des vulnérabilités techniques	☑ STD ☐ AVC ☐ REG
			PST.4.02.	Notification des mises à jour de sécurité	☑ STD ☐ AVC ☐ REG
			PST.4.03.	Contrôle de la fiabilité des mises à jour logicielles	☑ STD ☐ AVC ☐ REG
			PST.4.04.	Protection des secrets contenus dans les mises à jour logicielles	☑ STD ☐ AVC ☐ REG

PAD.	Protection de l'accès aux données				
	PAD.1.	Contrôle et cloisonnement des accès aux données			
			PAD.1.01.	Contrôle systématique de l'accès aux données sensibles	☑ STD ☐ AVC ☐ REG
			PAD.1.02.	Cloisonnement des accès aux données utilisateurs	☑ STD ☐ AVC ☐ REG
	PAD.2.	Authentification forte			
			PAD.2.01.	Support de dispositifs de soft-tokens ou hard-tokens	☐ STD ☑ AVC ☐ REG
	PAD.3.	Personnalisation des mots de passe et secrets			
			PAD.3.01.	Personnalisation systématique des mots de passe utilisateurs	☑ STD ☐ AVC ☐ REG
			PAD.3.02.	Définition des mots de passe techniques et des secrets lors de l'installation/configuration de la solution	☑ STD ☐ AVC ☐ REG
	PAD.4.	Sécurisation des procédures de gestion des mots de passe			
			PAD.4.01.	Non divulgation des attributs utilisateurs	☑ STD ☐ AVC ☐ REG
			PAD.4.02.	Contrôle d'identité préalable à la récupération de mot de passe	☑ STD ☐ AVC ☐ REG
			PAD.4.03.	Contrôle d'identité préalable à la modification de mot de passe	☑ STD ☐ AVC ☐ REG

PAD.5.	Stockage sécurisé des mots de passe et secrets				
		PAD.5.01.	Stockage des mots de passe sous forme de condensats ou chiffrés	☑ STD ☐ AVC	☐ REG
		PAD.5.02.	Robustesse des condensats	☑ STD ☐ AVC	☐ REG
		PAD.5.03.	Stockage des secrets dans un élément de sécurité	☐ STD ☑ AVC	☐ REG
PAD.6.	Effacement des données utilisateurs				
		PAD.6.01.	Dispositif de suppression des données utilisateurs	☑ STD ☐ AVC	☐ REG

TRA.	Traçabilité				
	TRA.1. Journalisation des événements				
		TRA.1.01.	Existence d'un journal des événements	☑ STD ☐ AVC	☐ REG
		TRA.1.02.	Imputabilité des événements journalisés	☐ STD ☑ AVC	☐ REG
	TRA.2. Protection des traces				
		TRA.2.01.	Contrôle des accès aux événements journalisés	☑ STD ☐ AVC	☐ REG

3. DESCRIPTION DES EXIGENCES DE SECURITE

3.1. Protection des échanges de données

Thème	PED 1.	Protection des échanges de données ➥Chiffrement des données		
Exigence	**PED 1.01**	**▸ Chiffrement des échanges de données sensibles**	**☑ STD ☐ AVC**	**☐ REG**
Description :	La confidentialité des données sensibles échangées via le(s) moyen(s) de communication mis en œuvre par la solution IoT doit être préservée par un dispositif de chiffrement conforme aux standards décrits ci-dessous pour chaque type de mécanisme de chiffrement retenu : symétrique ou asymétrique. Les algorithmes de chiffrement symétrique considérés comme standards doivent présenter les caractéristiques suivantes : - dans le cas d'algorithmes de chiffrement par bloc, la taille du bloc doit être au minimum de 128 bits et l'algorithme doit être largement éprouvé dans le milieu académique (tel AES) ; - dans le cas d'algorithmes de chiffrement par flux, celui-ci ne doit pas présenter de vulnérabilités permettant de le casser en moins de 2^{128} calculs. Les algorithmes de chiffrement asymétrique considérés comme standards doivent présenter les caractéristiques suivantes : - l'algorithme de chiffrement employé doit disposer d'une preuve de sécurité. L'utilisation de canaux de communication non chiffrés est acceptable à la condition que toutes les données sensibles y transitant soient elles-mêmes chiffrées.		
Périmètre :	Cette exigence s'applique à tout échange de données sensibles au moyen de la solution IoT, mais non à l'ensemble des données échangées.		

Thème	PED 1.	Protection des échanges de données ➥Chiffrement des données		
Exigence	**PED 1.02**	**▸ Chiffrement de tous les échanges de données**	**☐ STD ☑ AVC**	**☐ REG**
Description **:**	La confidentialité de toutes les données échangées via le(s) moyen(s) de communication mis en œuvre par la solution IoT doit être préservée par un dispositif de chiffrement conforme aux standards décrits ci-dessous pour chaque type de mécanisme de chiffrement retenu : symétrique ou asymétrique. Les algorithmes de chiffrement symétrique considérés comme standards doivent présenter les caractéristiques suivantes : - dans le cas d'algorithmes de chiffrement par bloc, la taille du bloc doit être au minimum de 128 bits et l'algorithme doit être largement éprouvé dans le milieu académique (tel AES) ; - dans le cas d'algorithmes de chiffrement par flux, celui-ci ne doit pas présenter de vulnérabilités permettant de le casser en moins de 2^{128} calculs. Les algorithmes de chiffrement asymétrique considérés comme standards doivent présenter les caractéristiques suivantes : - l'algorithme de chiffrement employé doit disposer d'une preuve de sécurité. Note : les systèmes de chiffrement de bout en bout sont fortement recommandés dans le cadre de cette exigence, car ils permettent d'assurer la sécurité du canal de communication indépendamment de la nature des données y transitant.		
Périmètre **:**	Cette exigence s'applique à tous les échanges de données au moyen de la solution IoT, quelle que soit leur sensibilité.			

Thème	PED 1.	Protection des échanges de données ➥Chiffrement des données		
Exigence	**PED 1.03**	**▸ Robustesse des clés de chiffrement**	**☑ STD ☐ AVC**	**☐ REG**
Description :	Le choix des clés chiffrement doit respecter les critères suivants : - les clés de chiffrement symétrique doivent avoir une taille minimale de 128 bits ; - les clés de chiffrement asymétrique doivent avoir une taille minimale de 3072 bits ; - les clés de chiffrement doivent être uniques par équipement et par utilisateur ; - les clés de chiffrement ne doivent pas être pas générées à partir de données publiques (numéros de série, adresses matérielles, etc.).			
Périmètre :	Cette exigence s'applique à tout mécanisme de génération de clés, qu'elles soient très temporaires (liées à une session par exemple) ou d'une durée d'utilisation plus longue.			

Thème	PED 2.	Protection des échanges de données ➥Contrôle d'intégrité des échanges		
Exigence	**PED 2.01**	**▸ Contrôle d'intégrité des échanges de données sensibles**	**☑ STD ☐ AVC**	**☐ REG**
Description :	L'intégrité des échanges de données sensibles réalisés dans le cadre de la solution IoT doit être assurée, notamment par un des mécanismes spécifiques suivants : - une somme de contrôle reconnue comme fiable, sa robustesse n'ayant pas été remise en cause (SHA256 ou équivalent) ; - une somme de contrôle cryptographique fiable (MAC) ; - un système de code correcteur d'erreur (EEC). Note : cette exigence ne concerne que le contrôle d'intégrité des échanges de données sensibles ; elle peut néanmoins être satisfaite par un mécanisme fournissant des garanties d'intégrité et d'authenticité tel que l'utilisation de sommes de contrôle cryptographiques ou de signatures asymétriques.		
Périmètre :	Cette exigence s'applique à tout échange de données sensibles au moyen de la solution IoT, mais non à l'ensemble des données échangées.		

Thème	PED 2.	Protection des échanges de données ➥Contrôle d'intégrité des échanges		
Exigence	**PED 2.02**	**▸ Contrôle d'intégrité de tous les échanges de données**	**☐ STD ☑ AVC**	**☐ REG**
Description :	L'intégrité de tous les échanges de données réalisés dans le cadre de la solution IoT doit être assurée par au moins un des mécanismes spécifiques suivants : - une somme de contrôle reconnue comme fiable, sa robustesse n'ayant pas été remise en cause (SHA256 ou équivalent) ; - une somme de contrôle cryptographique fiable (MAC) ; - un système de code correcteur d'erreur (EEC). Note : cette exigence ne concerne que le contrôle d'intégrité des échanges de données et non la vérification de l'authenticité des données ; elle peut néanmoins être satisfaite par un mécanisme fournissant des garanties d'intégrité et d'authenticité tel que l'utilisation de sommes de contrôle cryptographiques ou de signatures asymétriques.		
Périmètre :	Cette exigence s'applique à tous les échanges de données au moyen de la solution IoT, quelle que soit leur sensibilité.		

Thème	PED 2.	Protection des échanges de données ➥Contrôle d'intégrité des échanges		
Exigence	**PED 2.03**	**▸ Authentification mutuelle des échanges de données**	**☐ STD ☑ AVC**	**☐ REG**
Description :	Les échanges de données entre les différents composants de la solution IoT doivent être soumis à une authentification mutuelle au moyen de mécanismes reconnus comme fiables (leur robustesse n'ayant pas été remise en cause) tels que : - une somme de contrôle cryptographique ; - une signature numérique. Note : la grande majorité de ces mécanismes d'authentification assure par ailleurs l'intégrité des échanges.			
Périmètre :	Cette exigence s'applique aux protocoles de communication de tous types, dont certains proposent des mécanismes adaptés (tel TLS par exemple).			

Thème	PED 2.	Protection des échanges de données ➥Contrôle d'intégrité des échanges		
Exigence	**PED 2.04**	**▸ Non rejeu de tous les échanges de données**	**☑ STD ☐ AVC**	**☐ REG**
Description :	Les échanges de données entre les différents composants de la solution IoT doivent être protégés contre les attaques par rejeu au moyen de mécanismes reconnus comme fiables tels que : - l'authentification défi-réponse ; - Un mode d'opération de chiffrement adapté (EAX, CCM, GCM, etc.).			
Périmètre :	Cette exigence s'applique à tous les échanges de données au moyen de la solution IoT, quelle que soit leur sensibilité.			

3.2. Protection des socles techniques

Thème	PST 1.	Protection des socles techniques ➥Durcissement des configurations matérielles		
Exigence	**PST 1.01**	**▸ Protection des interfaces de débogage**	**☑ STD ☐ AVC**	**☐ REG**
Description :	L'accès aux interfaces de débogage doit être rendu extrêmement complexe pour une personne non autorisée (attaquant) du fait de : - la désactivation des fonctionnalités de débogage matérielles (activation d'un fusible) ; - la mise en place d'un contrôle par mot de passe restreignant l'accès aux interfaces de débogage. Le non-câblage des interfaces de débogage matérielles n'est pas suffisant, mais est considéré comme un plus si ces dernières sont rendues inaccessibles à un attaquant.			
Périmètre :	Cette exigence s'applique à tous les composants électroniques offrant une ou plusieurs interfaces de débogage matérielles : JTAG, SWD, etc.			

Thème	PST 2.	Protection des socles techniques ➥Protection physique des équipements		
Exigence	**PST 2.01**	**▸ Détection d'ouverture du boîtier**	**☐ STD ☑ AVC**	**☐ REG**
Description :	L'équipement doit posséder au moins un système de détection d'ouverture déclenchant une action de sécurité parmi les suivantes : - effacement de secrets des mémoires de stockage ; - envoi d'une alerte silencieuse par un canal de communication. L'équipement peut offrir le moyen aux personnes autorisées de désactiver le mécanisme de détection d'ouverture du boîtier (dans le cadre d'opérations de contrôle ou de maintenance par exemple), sous réserve de leur authentification préalable.			
Périmètre :	Cette exigence s'applique aux équipements matériels contenant des secrets ou des données sensibles.			

Thème	PST 3.	Protection des socles techniques ➥Durcissement des configurations logicielles		
Exigence	**PST 3.01**	**▸ Prise en compte des vulnérabilités publiées par l'OWASP**	**☑ STD ☐ AVC**	**☐ REG**
Description :	La configuration des interfaces et services web doit respecter les bonnes pratiques définies par l'Open Web Application Security Project (OWASP) concernant en particulier la prise en compte du *Top 10 des risques de sécurité* publié sur son site (www.owasp.org) et portant actuellement sur : - les vulnérabilités d'injection (injection de code SQL, de commandes, etc.) ; - les mécanismes d'authentification défaillants ; - l'exposition de données sensibles ; - les entités externes XML (XXE) ; - les mécanismes de contrôle d'accès défaillants ; - les erreurs de configuration ; - les injections de code par site tiers ; - la dé-sérialisation non sécurisée de contenu ; - l'utilisation de composants vulnérables ; - l'insuffisance/absence de journalisation.		
Périmètre :	Cette exigence s'applique uniquement aux interfaces web et aux applications mobiles ou bureau reposant sur des interfaces web (telles Cordova par exemple).		

Thème	PST 3.	Protection des socles techniques ➥Durcissement des configurations logicielles		
Exigence	**PST 3.02**	**▸ Restriction des services**	**☑ STD ☐ AVC**	**☐ REG**
Description :	Les services réseau exposés par les systèmes et les applications doivent être restreints aux seuls services nécessaires au bon fonctionnement de la solution.			
Périmètre :	Cette exigence s'applique aux équipements comportant des systèmes ou des applications utilisant le protocole IP.			

Thème	PST 4.	Protection des socles techniques ➥Maintien en conditions de sécurité		
Exigence	**PST 4.01**	**▸ Dispositif de correction des vulnérabilités techniques**	**☑ STD ☐ AVC**	**☐ REG**
Description :	Au moins un dispositif doit permettre de corriger les vulnérabilités logicielles publiées, via une mise à jour logicielle (prenant en compte logiciels et micro-logiciels). Il peut s'agir : - d'un système de déploiement de mises à jour (par connectique USB, carte mémoire ou *over-the-air*) ; - du remplacement de l'équipement faillible par un équipement disposant des logiciels et micro-logiciels mis à jour.			
Périmètre :	Cette exigence s'applique aux équipements matériels, aux applications mobiles reposant sur le système de déploiement d'application sous-jacent (iOS, Android, Blackberry, Windows Phone) et aux applications web hébergées dans le Cloud et étant à la charge du fournisseur de la solution IoT.			

Thème	PST 4.	Protection des socles techniques ➥Maintien en conditions de sécurité		
Exigence	**PST 4.02**	**▸ Notification des mises à jour de sécurité**	**☑ STD ☐ AVC**	**☐ REG**
Description :	Un dispositif de notification doit avertir l'utilisateur de la disponibilité de toute nouvelle mise à jour de sécurité dès lors qu'une action est requise de sa part pour sa mise en application au sein de la solution. Ce dispositif peut consister en : - une notification déclenchée par une application (mobile ou web) ; - l'envoi d'un courriel ou d'un SMS précisant la mise à disposition de la mise à jour ; - une notification lumineuse sur l'équipement. Le ou les mécanismes retenus doivent être proportionnés et suffisants à l'information de l'utilisateur. Ainsi, les adresses mails et numéros de téléphone utilisés pour notifier ce dernier doivent être régulièrement vérifiés. L'utilisation conjointe de plusieurs de mécanismes est fortement recommandée.		
Périmètre :	Cette exigence s'applique aux équipements matériels, aux applications mobiles reposant sur le système de déploiement d'application sous-jacent (iOS, Android, Blackberry, Windows Phone).		

Thème	PST 4.	Protection des socles techniques ➥Maintien en conditions de sécurité		
Exigence	**PST 4.03**	**▸ Contrôle de la fiabilité des mises à jour logicielles**	**☑ STD ☐ AVC**	**☐ REG**
Description :	Un dispositif de contrôle doit être mis en œuvre afin de vérifier la fiabilité des mises à jour logicielles applicables à la solution IoT. Il peut reposer sur : - un mécanisme de transmission incluant une authentification mutuelle (authentification par certificat client et serveur par exemple) ; - un mécanisme de signature à clé publique.		
Périmètre :	Cette exigence s'applique à tous les logiciels composant la solution, y compris ceux intégrés aux équipements, qui peuvent être mis à jour par quelque moyen que ce soit, tels que : - logiciels et micro-logiciels à destination de microcontrôleurs et System-on-Chip ; - applications mobiles et de bureau ; - systèmes d'exploitation embarqués.		

Thème	PST 4.	Protection des socles techniques ➥Maintien en conditions de sécurité		
Exigence	**PST 4.04**	**▸ Protection des secrets contenus dans les mises à jour logicielles**	**☑ STD ☐ AVC**	**☐ REG**
Description :	Le contenu des mises à jour logicielles doit être rendu inintelligible dès lors qu'il comprend des secrets dont la divulgation pourrait remettre en cause la sécurité de la solution IoT. Les dispositifs mis en œuvre pour ce faire peuvent reposer sur l'utilisation de mécanismes de chiffrement conformes aux exigences PED.1.X du présent référentiel.			
Périmètre :	Cette exigence s'applique à tous les logiciels composant la solution, y compris ceux intégrés aux équipements, dont les mises à jour sont susceptibles de contenir des secrets (clés de chiffrement, algorithmes, paramètres de configuration…).			

3.3. Protection de l'accès aux données

Thème	PAD 1.	Protection de l'accès aux données ➥Contrôle et cloisonnement des accès aux données		
Exigence	**PAD 1.01**	**▸ Contrôle systématique de l'accès aux données sensibles**	**☑ STD ☐ AVC**	**☐ REG**
Description :	Les données sensibles doivent être systématiquement protégées par un dispositif de contrôle d'accès : - constitué au minimum d'un dispositif d'authentification ; - complété éventuellement d'un système de gestion de droits d'accès. Aucune donnée sensible ne doit être accessible publiquement.			
Périmètre :	Cette exigence s'applique aux applications mobiles, web et de bureau, ainsi qu'aux services web afférents.			

Thème	PAD 1.	Protection de l'accès aux données ➥Contrôle et cloisonnement des accès aux données		
Exigence	**PAD 1.02**	**▸ Cloisonnement des accès aux données utilisateurs**	**☑ STD ☐ AVC**	**☐ REG**
Description :	Les accès aux données de chaque utilisateur doivent être restreints à ce dernier et aux applications qui les manipulent.			
Périmètre :	Cette exigence s'applique aux applications mobiles, web et de bureau, ainsi qu'aux services web afférents.			

Thème	PAD 2.	Protection de l'accès aux données ➥Authentification forte		
Exigence	**PAD 2.01**	**▸ Support de dispositifs de soft-tokens ou de hard-tokens**	**☐ STD ☑ AVC**	**☐ REG**
Description :	La solution doit supporter la mise en œuvre d'un dispositif d'authentification forte, reposant sur des *tokens* générés par un système dédié, qu'il s'agisse de matériel spécifique (ex : RSA-SecurID) ou de logiciel (ex : Google Authenticator). L'utilisateur doit être informé de l'existence de ce dispositif et être en capacité : - d'activer et de désactiver l'authentification à deux facteurs ; - de gérer ses tokens (création, révocation).			
Périmètre :	Cette exigence s'applique aux applications mobiles, web et de bureau.			

Thème	PAD 3.	Protection de l'accès aux données ➥Personnalisation des mots de passe et secrets		
Exigence	**PAD 3.01**	**‣ Personnalisation systématique des mots de passe utilisateurs**	**☑ STD ☐ AVC**	**☐ REG**
Description :	La solution doit imposer à l'utilisateur la définition ou la modification du (ou des) mots de passe assurant la protection des socles techniques ou des applications dès leur phase de configuration. L'utilisateur doit être alerté par la solution sur la nécessité de choisir des mots de passe robustes en respectant notamment les principes suivants : - le mot de passe doit être complexe (non trivial ni facile à deviner) ; - le mot de passe doit si possible être unique au service dont il contrôle l'accès.			
Périmètre :	Cette exigence s'applique à tous les composants de la solution utilisant un mot de passe, en particulier s'il est préconfiguré.			

Thème	PAD 3.	Protection de l'accès aux données ➥Personnalisation des mots de passe et secrets		
Exigence	**PAD 3.02**	**‣ Définition des mots de passe techniques et des secrets lors de l'installation/configuration de la solution**	**☑ STD ☐ AVC**	**☐ REG**
Description :	La solution doit utiliser des mots de passe techniques et des secrets uniques à chaque équipement, notamment en : - les provisionnant en sortie de chaîne de production ; - les générant lors de la phase d'installation ou de configuration ; - les téléchargeant à partir d'un service en ligne et en les installant dans l'équipement.			
Périmètre :	Cette exigence s'applique à tous les composants de la solution utilisant des mots de passe techniques ou des secrets, en particulier s'ils sont préconfigurés.			

Thème	PAD 4.	Protection de l'accès aux données ➥Sécurisation des procédures de gestion des mots de passe		
Exigence	**PAD 4.01**	**‣ Non divulgation des attributs utilisateurs**	**☑ STD ☐ AVC**	**☐ REG**
Description :	Les dispositifs permettant de solliciter la récupération ou le renouvellement des mots de passe utilisateurs (en cas d'oubli notamment) ne doivent pas permettre d'obtenir d'informations susceptibles d'être utilisées à des fins d'accès illicite à la solution, telles que : - le nom d'utilisateurs ; - l'adresse de courriels d'utilisateurs.			
Périmètre :	Cette exigence s'applique à toute interface permettant de gérer un compte utilisateur.			

Thème	PAD 4.	Protection de l'accès aux données ➥Sécurisation des procédures de gestion des mots de passe		
Exigence	PAD 4.02	▸ Contrôle d'identité préalable à la récupération de mot de passe	☑ STD ☐ AVC	☐ REG
Description :		Les dispositifs permettant la récupération ou le renouvellement des mots de passe utilisateurs (en cas d'oubli notamment) doivent vérifier l'identité des utilisateurs à l'origine de cette demande par des moyens tels que : - envoi d'un SMS contenant un code de vérification (dans le cas où le numéro de téléphone de l'utilisateur a été préalablement enregistré et conservé par le fournisseur du service) ; - envoi d'un courriel contenant un lien à usage unique permettant le renouvellement du mot de passe (si l'adresse de courriel de l'utilisateur a été préalablement enregistrée et conservée par le fournisseur du service) ; - vérification de la réponse à une question secrète préalablement définie par l'utilisateur. Si l'identité de l'utilisateur ne peut pas être vérifiée, un mécanisme de réinitialisation de mot de passe par accès local à l'équipement peut être mis en œuvre, sous condition qu'il entraine la suppression des données sensibles.		
Périmètre :		Cette exigence s'applique à toute interface permettant de gérer un compte utilisateur.		

Thème	PAD 4.	Protection de l'accès aux données ➥Sécurisation des procédures de gestion des mots de passe		
Exigence	PAD 4.03	▸ Contrôle d'identité préalable à la modification de mot de passe	☑ STD ☐ AVC	☐ REG
Description :		Les dispositifs permettant la modification des mots de passe doivent vérifier l'identité des utilisateurs sollicitant cette opération par un des moyens suivants : - saisie du mot de passe actuel par l'utilisateur et vérification ; - envoi d'un SMS contenant un code de vérification (dans le cas où le numéro de téléphone de l'utilisateur a été préalablement enregistré et conservé).		
Périmètre :		Cette exigence s'applique à toute interface permettant de gérer un compte utilisateur.		

Thème	PAD 5.	Protection de l'accès aux données ➥Stockage sécurisé des mots de passe et secrets		
Exigence	**PAD 5.01**	**▸ Stockage des mots de passe sous forme de condensats ou chiffrés**	**☑ STD ☐ AVC**	**☐ REG**
Description :		La confidentialité et l'usage légitime des mots de passe devant impérativement être préservés, les précautions ci-dessous doivent être appliquées. Dans le cas où une application a besoin uniquement de vérifier la connaissance d'un mot de passe, cette dernière ne doit stocker qu'un condensat du mot de passe, résultant d'une opération de condensation (*hashage*) de ce dernier et respectant l'exigence PAD.5.02 du présent référentiel. Dans le cas où une application a besoin de réutiliser un mot de passe et uniquement dans ce cas (pour des opérations d'authentification principalement), ce dernier peut être stocké de façon chiffrée, sous condition du respect des dispositions requises par les exigences PED.1.X du présent référentiel. La réversibilité du chiffrement permet alors retrouver le mot de passe sous réserve de détenir la clé adéquate, tout en assurant sa confidentialité.		
Périmètre :		Cette exigence s'applique à toute application stockant un mot de passe ou son condensat sur quelque support que ce soit (base de données, système de fichiers, mémoire…), incluant notamment : - les applications mobiles ; - les micro-logiciels ; - les logiciels déployés au sein d'équipements pouvant être physiquement compromis.		

Thème	PAD 5.	Protection de l'accès aux données ➥Stockage sécurisé des mots de passe et secrets		
Exigence	**PAD 5.02**	**‣ Robustesse des condensats**	**☑ STD ☐ AVC**	**☐ REG**
Description :	Les mécanismes de génération des condensats de mots de passe doivent présenter les caractéristiques suivantes : - la taille minimale des condensats générés est de 256 bits ; - la meilleure attaque connue permettant de trouver des collisions doit nécessiter de l'ordre de $2^{h/2}$ calculs de condensats, où *h* désigne la taille en bit du condensat ; - l'utilisation d'un grain de sel est obligatoire, afin de ne pas dévoiler d'information en cas de compromission ; - le nombre d'itérations doit être conforme à l'état de l'art en cas de calcul de condensat itératif (ex : bcrypt, scrypt ou PBKDF2). Note : les algorithmes de hashage tels SHA-256 ou SHA-512 sont conformes à cette exigence.		
Périmètre :	Cette exigence s'applique à tout logiciel effectuant un calcul de condensat sur des données sensibles.		

Thème	PAD 5.	Protection de l'accès aux données ➥Stockage sécurisé des mots de passe et secrets		
Exigence	**PAD 5.03**	**‣ Stockage des mots de passe dans un éléments de sécurité**	**☐ STD ☑ AVC**	**☐ REG**
Description :	Afin de préserver la sécurité des fonctions cryptographiques, les secrets utilisés dans l'équipement doivent être enfouis au sein d'un élément de sécurité (HSM, Hardware Security Module) reconnu (Critères Communs, FIPS 140).			
Périmètre :	Cette exigence s'applique à tous les équipements de la solution IoT utilisant des fonctions cryptographiques.			

Thème	PAD 6.	Protection de l'accès aux données ➥Effacement des données utilisateurs		
Exigence	**PAD 6.01**	**‣ Dispositif de suppression des données utilisateurs**	**☑ STD ☐ AVC**	**☐ REG**
Description :	Une fonctionnalité de suppression définitive des données utilisateurs doit permettre leur effacement sans rendre inopérant l'application ou l'équipement qui les utilisait.			
Périmètre :	Cette exigence s'applique à tous les équipements et applications stockant des données utilisateurs.			

3.4. TRAÇABILITE

Thème	TRA 1.	Traçabilité ➥Journalisation des événements		
Exigence	TRA 1.01	▸ Existence d'un journal des événements	☑ STD ☐ AVC	☐ REG
Description :	Un journal des événements doit être alimenté en continu fournissant au minimum les traces informatiques permettant : - de connaitre la nature des opérations réalisées dans le cadre fonctionnel de la solution ; - de dater ces opérations. En aucun cas ces traces ne doivent mentionner le contenu de secrets, mots de passe, ou toute autre information dont la confidentialité doit être préservée.			
Périmètre :	Cette exigence s'applique aux équipements et aux applications composant la solution IoT.			

Thème	TRA 1.	Traçabilité ➥Journalisation des événements		
Exigence	TRA 1.02	▸ Imputabilité des événements journalisés	☐ STD ☑ AVC	☐ REG
Description :	Les traces informatiques générées par la solution doivent permettre d'imputer les événements journalisés (opérations ou tentatives d'opérations) à leur origine (personnes physiques, équipements techniques, application…).			
Périmètre :	Cette exigence s'applique aux équipements et aux applications composant la solution IoT.			

Thème	TRA 2.	Traçabilité ➥Protection des traces		
Exigence	TRA 2.01	▸ Contrôle des accès aux événements journalisés	☑ STD ☐ AVC	☐ REG
Description :	Les traces informatiques inscrites dans les journaux d'événements doivent être protégées par un dispositif de contrôle d'accès.			
Périmètre :	Cette exigence s'applique à l'ensemble des journaux d'événements alimentés par les différents composants de la solution.			

4. GLOSSAIRE

Données sensibles :	Les données considérées comme « sensibles » dans le cadre du présent référentiel d'exigences sont les données à caractère personnel, les données qualifiées de sensibles par le RGPD, l'ensemble les données soumises à une réglementation sectorielle (données de santé, données bancaires, données financières, etc.) et les données de pilotage distant de la solution IoT. Les secrets utilisés dans le cadre de la solution IoT sont également des données considérées comme « sensibles ».
Secrets :	Les secrets regroupent les certificats et les clés utilisés dans un contexte cryptographique.
Mots de passe techniques :	Tout mot de passe utilisé par la solution IoT non destiné à ses utilisateurs est considéré comme un mot de passe technique.