

SECURITY BY DESIGN

Tekin

14 OCTOBRE 2025



QUI SOMMES NOUS ?

Depuis 2014, TEKIN conçoit, développe et déploie des solutions techniques à forte valeur ajoutée, pour les secteurs de l'industrie, énergie, santé, et infrastructures critiques.

ENGINEERING

Accompagnement, conseil et ingénierie sur les projets IoT

HARDWARE

Conception de systèmes IoT (électronique et logiciels embarqués)

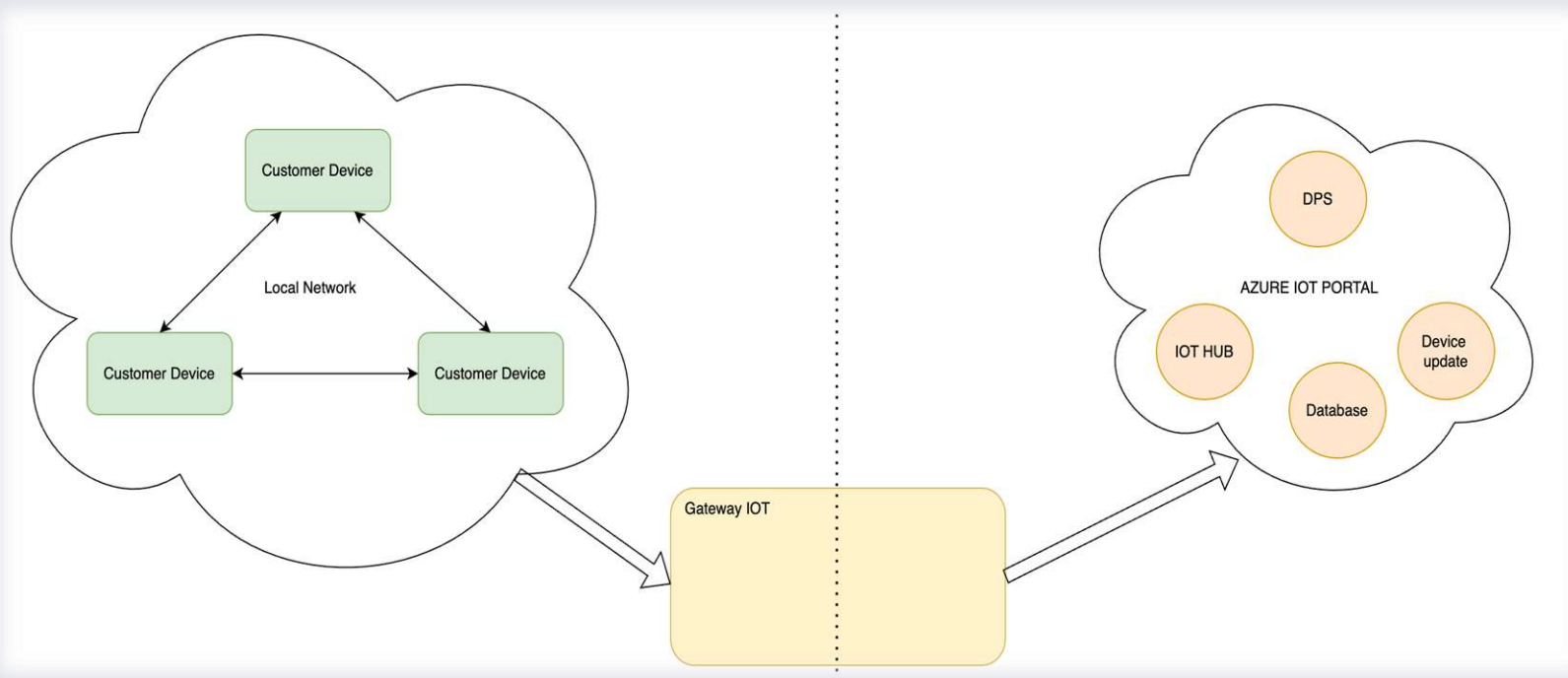
SOFTWARE

Développement d'applications web, mobile, desktop

CLOUD

Architectures cloud, déploiement valorisation des data

CONTEXTE ET OBJECTIFS



Remonter les données de dispositifs médicaux



Assurer la sécurisation des données via AZURE (backend)



Garantir une communication unidirectionnelle (capteurs → cloud)

RÉFÉRENTIELS NORMATIFS



IEC 62443-4-2

- ✓ Défense en profondeur
- ✓ Intégrité du logiciel
- ✓ Identité unique par équipement
- ✓ Supervision continue



ENISA IoT security baseline

- ✓ Principes de conception sécurisée et d'évaluation du risque IoT.



ANSSI

- ✓ Recommandations relatives à la sécurité des objets connectés
- ✓ Recommandations de configuration d'un système Linux

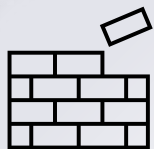
MATRICE DE RISQUES/IMPACTS

		Impacts			
Risques	Compromission d'une clé de connexion	Contrôle du parc ou de l'appareil	Usurpation d'identité		
	Falsification de l'appareil	Perte de confiance	Risques de clones	Augmentation de la charge cloud	
	Exploitation de failles logicielles	Exécution de code malveillant	Compromission applicative	Usurpation des données	Détournement de fonctionnement
	Man in the middle	Vol de données	Altération des données		
	Intrusion physique	Accès au système	Détournement de fonctionnement	Récupération des clés	

MATRICE DE RISQUES/PRÉCONISATIONS

	préconisations			
Risques	Compromission d'une clé de connexion	Stockage dans OP-TEE/TPM	Tokens à durée de vie courte et renouvelés automatiquement	
	Falsification de l'appareil	Provisionnement par DPS	Clés uniques par devices	Outils de production
	Exploitation de failles logicielles	Patching régulier	Revue et outils de vérification de code	Mise à jour
	Man in the middle	TLS mutualisé	Mise à jour des certificats	Anti-replay
	Intrusion physique	Ports de débogage désactivés	Tamper hardware	Secure Boot

PRÉCONISATIONS GLOBALES



Sécurisation du système embarqué via cloisonnement des environnements (OP-TEE)

Supervision et journalisation

Chiffrement des communications via TLS

Réduction de la surface d'attaque

Maintenance du système

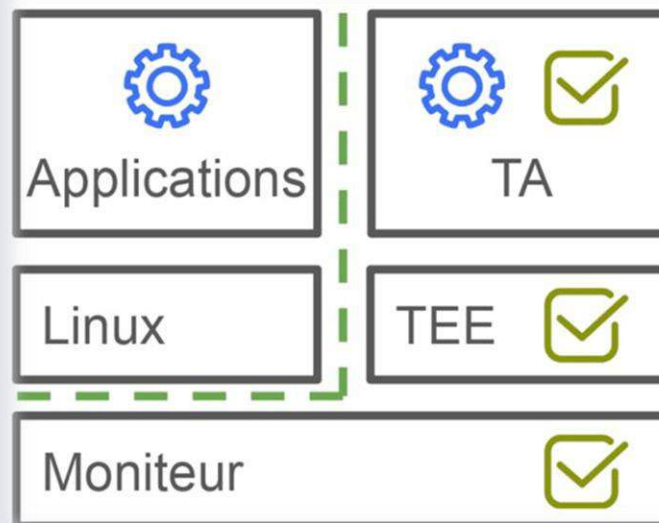
ENVIRONNEMENT DE CONFIANCE (TRUSTZONE)

Stockage des secrets
en zone sécurisé

-> clés jamais exposées



Utilisation d'un espace
mémoire de confiance
(OP-TEE sur ARM/TPM)



Génération locale
de tokens à
validité limitée



Séparation du logiciel
métier (linux standard)
et les secrets (zone de
confiance)

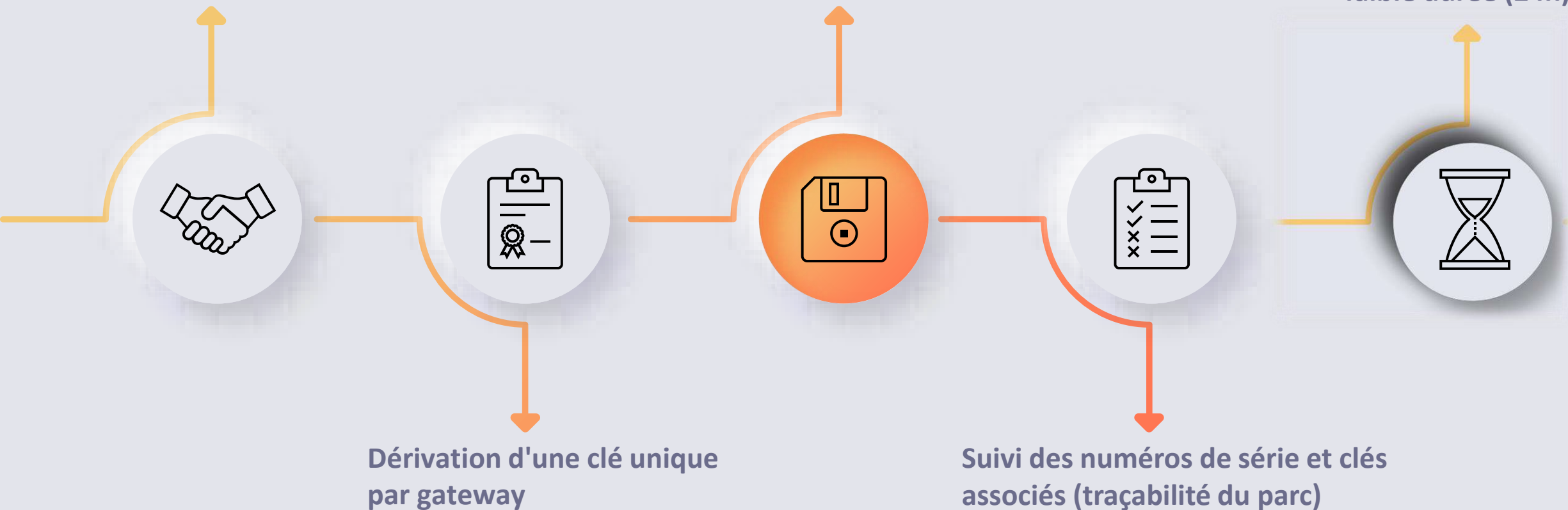


GESTION DU CYCLE DES CLÉS

Gestion du provisionnement via le DPS (device provisioning service) d'AZURE

Stockage de la clé en zone sécurisée en production

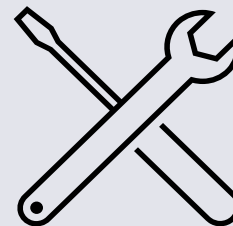
Création de tokens de faible durée (24h)



CHAQUE GATEWAY DISPOSE D'UNE IDENTITÉ DÉRIVÉE ET VÉRIFIABLE, ASSURANT L'AUTHENTICITÉ DU PARC COMPLET.

CONTRÔLE D'ACCÈS PHYSIQUES

Authentification via clé privée



Ports debug uniquement en accès interne via port TTL uniquement, désactivable en production

Log des connexions, journalisation et envoi des données d'alertes



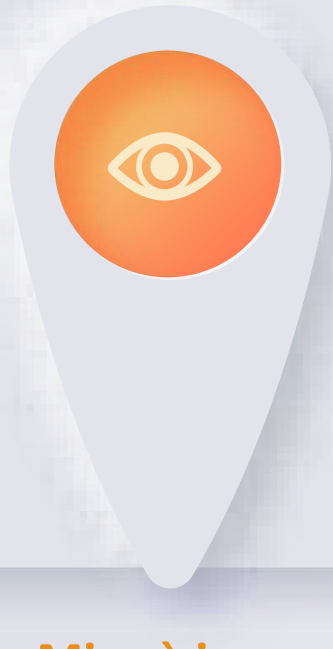
Détection des tentatives d'intrusion via Tamper hardware

CYCLE DE VIE DU PRODUIT



Production

- ✓ Chaîne de build maîtrisée (hash/signature)
- ✓ Injection des secrets en zone mémoire sécurisée
- ✓ Suivi de production et traçabilité du parc



Mise à jour

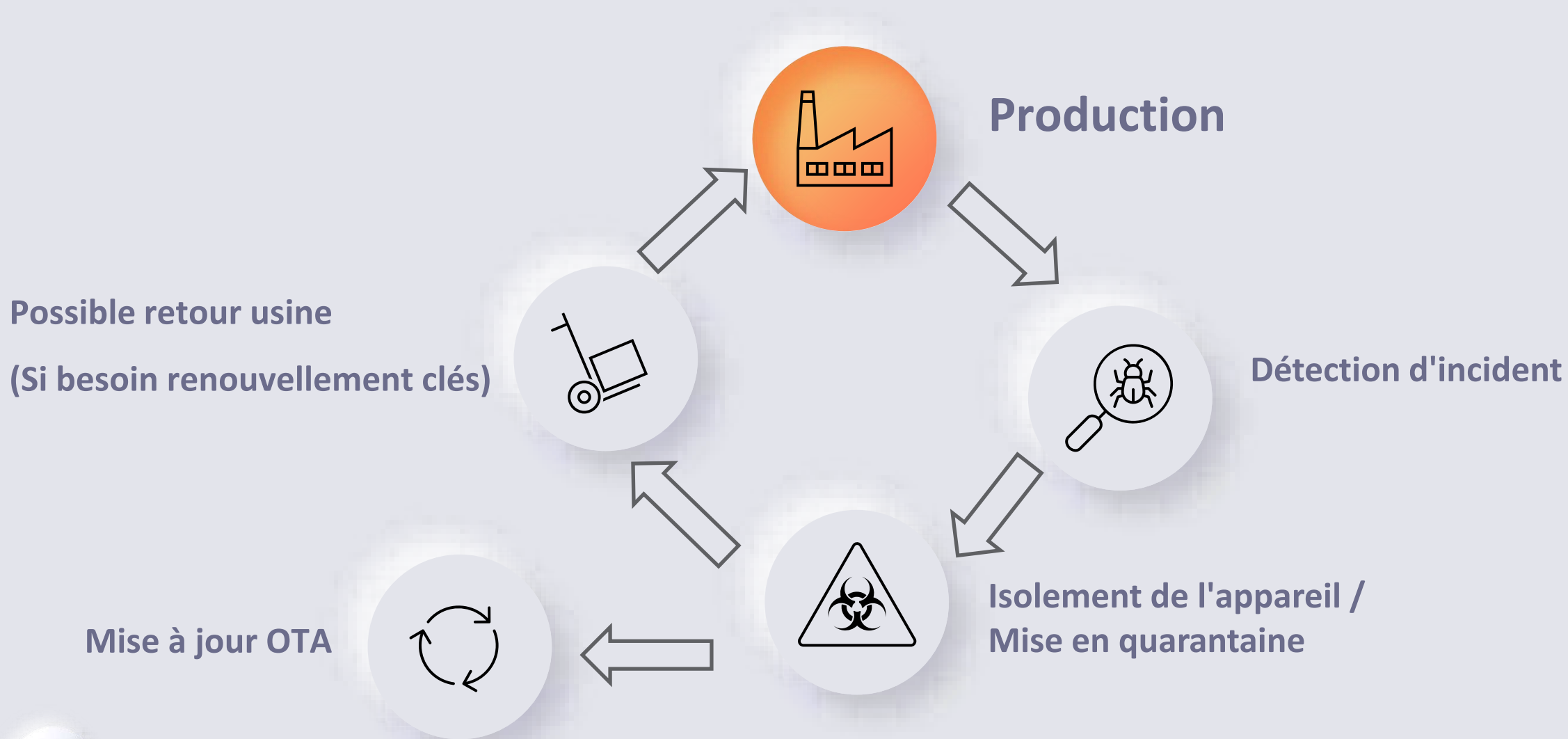
- ✓ Paquet de mise à jour vérifié (hash/signature)
- ✓ Vérification de l'intégrité avant déploiement
- ✓ Rollback en cas d'échec (système de partition A/B)
- ✓ Suivi du parc



Maintenance

- ✓ Journalisation des événements
- ✓ Alertes cloud en cas d'erreurs/événements suspects

GESTION D'INCIDENTS



IMPLÉMENTATION DANS NOTRE GATEWAY



Authentification et clés

- Clés dérivées issues du DPS AZURE
- Tokens SAS renouvelés automatiquement toutes les 24 h
- Clés et génération de token intégralement dans le OP-TEE (ARMv8 Secure World)



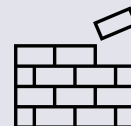
Impact sur les performances

- Environ 5 à 10% de consommation CPU/RAM supplémentaire



Chiffrement des communications

- Protocole MQTT sur TLS 1.3 avec CA DigiCert Global G2 intégré à Linux



Architecture sur STM32MP257

- Séparation des logiciels (métier et sécurisation)
- Intégration d'un agent de mise à jour (Azure Device Update & Swupdate)

CONCLUSION



Analyse

Analyse des risques et préconisations
(cartographie du système)



Design

Protection et gestion des secrets.

Réduire la surface d'attaque



Suivi du parc

Suivi sur tout le cycle de vie du produit
(production/exploitation/évolutions)



Gestion d'incidents

Capacité de réaction
(révocation, gestion des incidents)

UN IOT SÉCURISÉ REPOSE SUR LA CONFIANCE, LA MAÎTRISE DU CYCLE DE VIE ET LA CAPACITÉ À RÉAGIR AUX INCIDENTS.