Mobile Access de dormakaba

Livre blanc

Pour les responsables de la sécurité informatique

Sécurité avec Mobile Access

dormakaba

Généralités

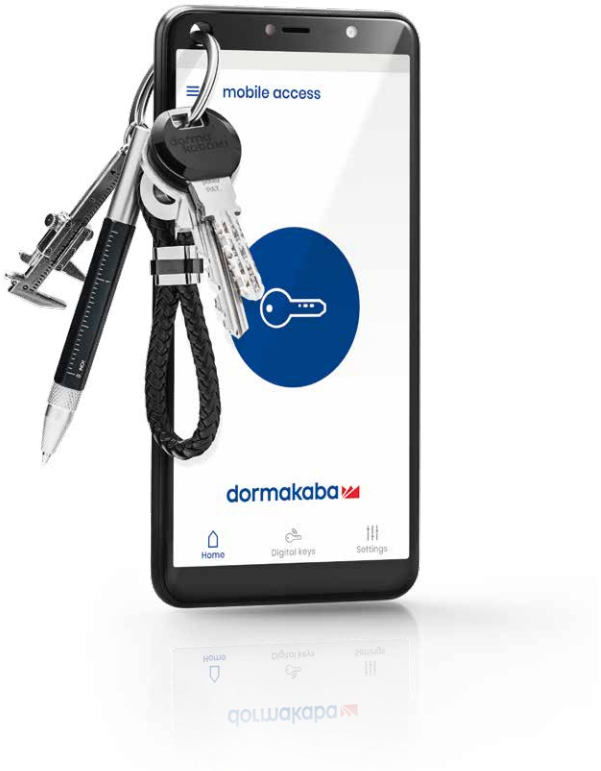
Avantages de Mobile Access

Avec Mobile Access, il est possible d'ouvrir des portes avec le smartphone. Le smartphone élargit ainsi la gamme de médias d'accès comprenant des clés et des badges (médias RFID).
Les droits d'accès peuvent être transférés sur un smartphone sans restriction temporelle ou géographique. Si une personne se tient devant une porte verrouillée, elle peut se voir accorder le droit d'accès sans nécessiter de support physique (clé, badge). Cela permet également de réduire les coûts de processus.

Groupe cible du présent document

Ce document est destiné spécifiquement aux utilisateurs du système suivants :

- **Responsables de la sécurité informatique**



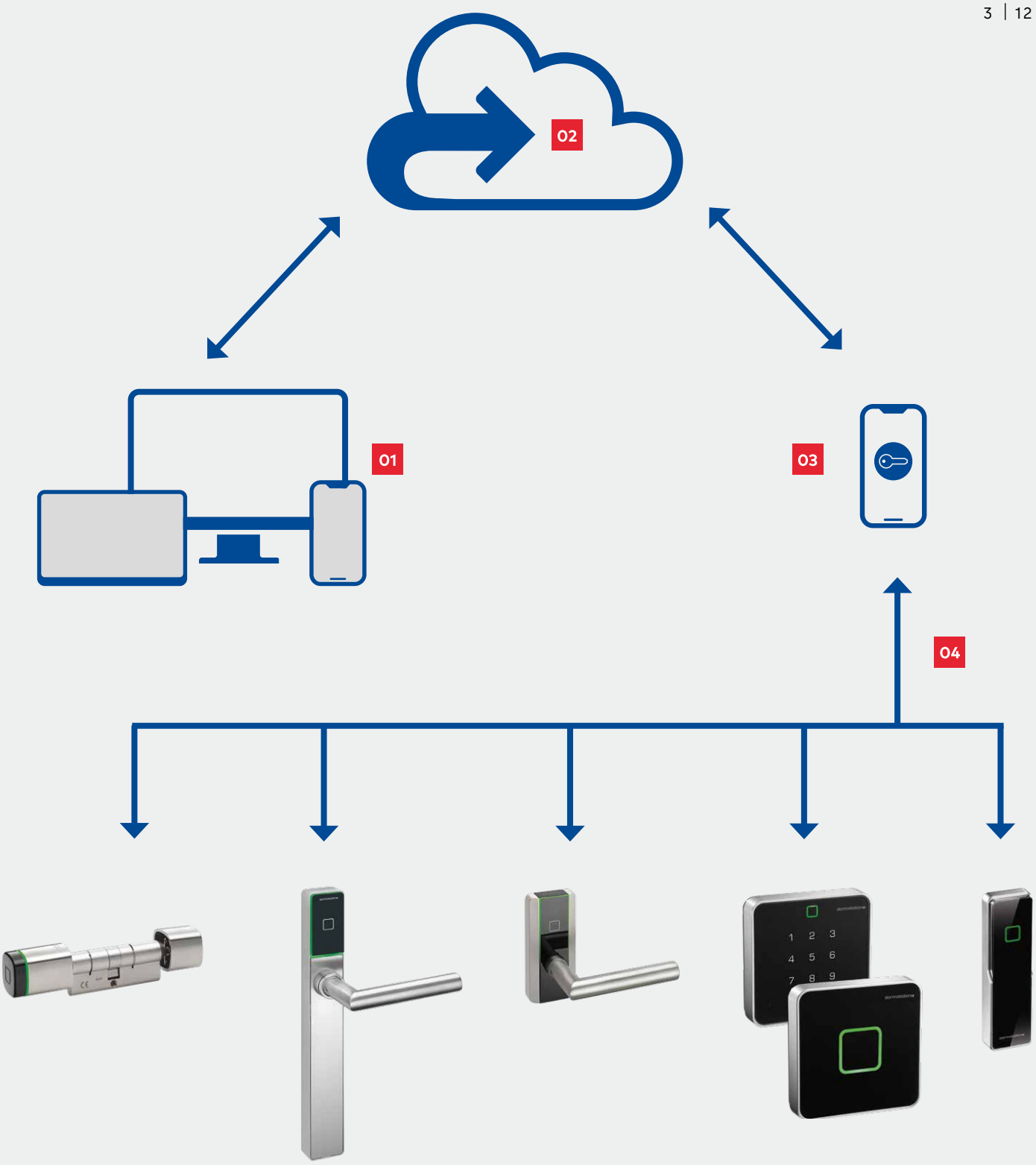
Structure du présent document

Le contenu de ce document est divisé en deux chapitres :

- **Architecture de sécurité Mobile Access :**
  Ce chapitre offre une vue d'ensemble des concepts de sécurité de base et décrit les aspects de sécurité pertinents sous forme d'introduction ou d'aperçu

- **Des questions concrètes concernant la sécurité du point de vue du responsable de la sécurité informatique :**
  Dans ce chapitre, nous évoquons des questions potentielles au sujet de la sécurité et y apportons des réponses, ainsi les différents aspects pourront être examinés sous différents angles

Certaines informations figurent à la fois dans le chapitre Vue d'ensemble et en tant que réponses à des questions (parfois à plusieurs questions), pour cette raison ces informations sont parfois disponibles plusieurs fois. La redondance de ces informations dans le document est délibérément prise en compte afin de pouvoir résumer les informations nécessaires dans le chapitre Vue d'ensemble et pour pouvoir apporter directement les réponses appropriées à toutes les questions.



Composants de la solution Mobile Access dormakaba

Mobile Access de dormakaba est supporté par les composants suivants :
Dans la solution d'accès **(1)** les droits d'accès sont attribués par la génération d'une clé digitale qui est transmise directement sur le smartphone via une plateforme sécurisée **(2)**. L'accès aux composants de portes **(4)** est alors possible avec le smartphone et l'application dormakaba mobile access. La communication entre le smartphone **(3)** et le composant de porte **(4)** peut s'effectuer via NFC (Near Field Communication) ou Bluetooth®.

Architecture de sécurité Mobile Access

La technologie LEGIC est utilisée pour la transmission sécurisée des clés digitales. Cela permet une transmission chiffrée (sécurisée contre toute manipulation et protégée contre l'interception) sur toute la distance :

- **de la solution d'accès de niveau supérieur/assurant la commande**
- **via le cloud**
- **via le smartphone**
- **jusqu'au composant de porte évaluant.**

Cryptage de bout en bout

L'élément principal est le chiffrement End2End des informations à protéger (clés digitales) du cloud au composant de porte, ce qui signifie notamment :

- Chiffrement dans le cloud :
  - Les clés de chiffrement requises ne sont disponibles que dans le cloud (elles sont stockées dans un environnement matériel sécurisé appelé Hardware Security Module/HSM - module de sécurité matériel).
- Transmission chiffrée du cloud vers le smartphone :
  - Les informations sont chiffrées sur le smartphone, les clés de déchiffrement ne sont pas présentes sur le smartphone, ce qui signifie que les informations (clés digitales) ne peuvent être ni lues, ni évaluées, ni modifiées.
- Transmission du smartphone au composant de porte de manière chiffrée (explicitement lors de la tentative d'accès) :
  - Déchiffrement dans une zone protégée (puce LEGIC) dans le composant de porte, les clés de déchiffrement sont disponibles dans le composant de porte dans une zone protégée (puce LEGIC). Les informations chiffrées sont utilisées temporairement pour décider des accès, puis supprimées.

Les différentes interfaces utilisent également des mesures de chiffrement/protection :

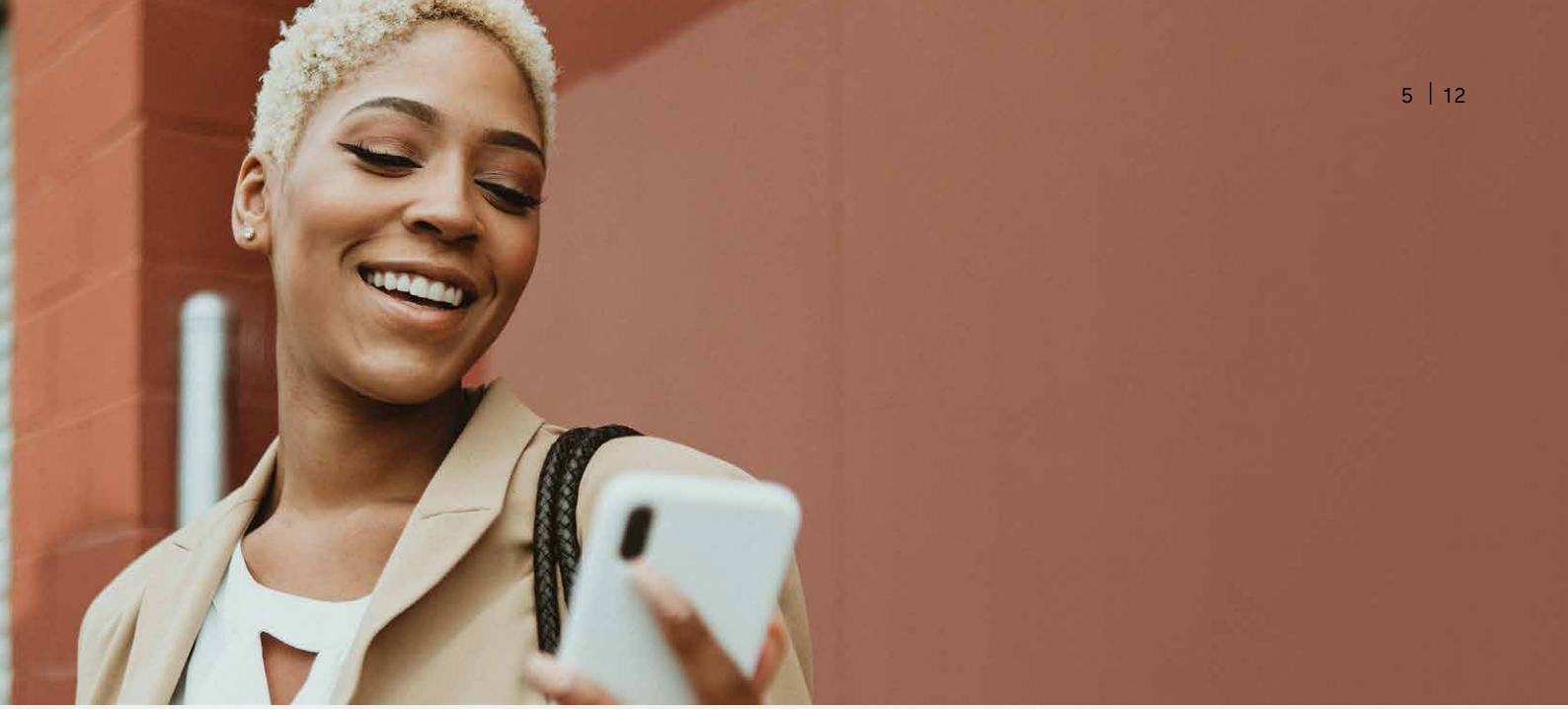
- Solution d'accès ⟷ Cloud (LEGIC Trusted Service): Communication chiffrée : HTTPS over TLS
- Cloud (LEGIC Trusted Service) ⟷ Smartphone : Communication chiffrée : HTTPS over TLS, Certificate pinning
- Smartphone – Composant de porte (puce LEGIC) : Mutual Authentication avec les clés de session AES128, de nouvelles clés de session pour chaque session

Clé de chiffrement/déchiffrement

Les clés de chiffrement/déchiffrement sont générées dans le module de sécurité matériel/HSM du cloud LEGIC sous forme de clés aléatoires.
Les clés de chiffrement/déchiffrement des informations sensibles (clés digitales) sont spécifiques à un projet, c'est-à-dire spécifique à chaque installation. Une installation couvre généralement le contrôle d'accès d'une entreprise ou d'un site. L'utilisation des clés de chiffrement/déchiffrement spécifiques au projet permet d'utiliser les mêmes clés digitales pour Mobile Access au sein d'une installation (par ex., dans une entreprise) ainsi que sur les médias RFID. D'autre part, cela empêche les clés digitales d'une entreprise d'être utilisées par une autre entreprise/indépendante.
Les clés de chiffrement/déchiffrement sont générées via le cloud (Trusted Service de la plate-forme LEGIC), qui génère ces clés de manière sécurisée dans un module de sécurité matériel (HSM) dans un environnement de sécurité certifié. Ces clés ne sortent jamais du HSM sous forme non chiffrée.
La transmission des clés requises (pour le chiffrement/déchiffrement) dans la zone protégée (puce LEGIC) du composant de porte se fait lors de la mise en service. Pour cela, les clés de déchiffrement nécessaires sont d'une part chiffrées et protégées par divers autres mécanismes de sécurité et, d'autre part, regroupées dans un pack, dénommé pack de configuration. La transmission de ces packs de configuration s'effectue indépendamment de l'application d'accès via une autre application, cette transmission est protégée par mot de passe.

Résumé

- Des clés aléatoires sont utilisées pour le chiffrement/déchiffrement.
- Ces clés aléatoires ne sortent jamais du HSM du cloud LEGIC sous une forme non protégée (plain).
- Pour la transmission des clés requises, celles-ci sont à leur tour chiffrées dans un package de configuration et protégées par divers autres mécanismes de sécurité.



Types de clés digitales

On distingue deux types de clés digitales qui correspondent à différents modèles d'autorisation :

- Infini-ID:
  Comprend un numéro identifiant le smartphone/la personne ; est unique pour chaque smartphone par projet. Le modèle d'autorisation avec Infini-ID est particulièrement adapté aux lecteurs Online et aux composants Wireless, car les autorisations peuvent être mises à jour directement sur ces derniers (en raison des connexions Online ou Wireless existantes).
- Infinilink:
  Comprend les règles d'accès d'une personne pour exactement un composant de porte. Une personne possède une clé Infinilink indépendante pour chaque porte autorisée, qui est visible dans l'application dormakaba mobile access.
  Les clés Infinilink ont une validité limitée et sont donc mises à jour par la solution d'accès assurant la commande en temps voulu avant expiration de la validité (clé Infinilink avec validité étendue). Une fois la validité expirée, aucun accès n'est possible. Le modèle d'autorisation avec Infinilink est particulièrement adapté aux composants standalone, car les personnes sont en possession des autorisations et aucune mise à jour manuelle des composants standalone n'est nécessaire en cas de modification des autorisations.
  Le verrouillage ou la suppression est effectué soit en supprimant la clé Infinilink du smartphone ou en l'ajoutant à la liste noire du composant de porte.

Informations supplémentaires sur le smartphone

En plus des contenus de la clé digitale, des informations supplémentaires sont transférées à une telle clé digitale de la solution d'accès via le cloud vers le smartphone, qui ne sont pas soumises au chiffrement End2End. Ces informations sont chiffrées sur toutes les interfaces de communication pertinentes, mais sont disponibles sur le smartphone avec de l'application dormakaba mobile access. Voici quelques exemples :

- Nom de la clé digitale/n° de smartphone pour Infini-ID ou le nom de porte pour Infinilink
- Temps d'attribution de la clé digitale
- Période de validité de la clé digitale (Infinilink), mais pas les autorisations/règles temporelles détaillées de la clé digitale chiffrée
- Nom de l'entreprise

Ces informations supplémentaires sont utilisées dans l'application dormakaba mobile access pour pouvoir visualiser des informations sur les clés digitales. L'utilisateur peut visualiser ces informations dans l'appli dormakaba mobile access pour chaque clé digitale. Ces informations supplémentaires ne seront pas utilisées pour la décision d'accès. La manipulation de ces informations ne modifiera donc pas les autorisations et, en particulier, ne permettra pas d'accès non autorisé.

Questions spécifiques concernant la sécurité du point de vue du responsable de la sécurité informatique

Quels sont les chiffrements utilisés entre les différents composants ?

Sur les interfaces de communication entre les différents composants impliqués, les mécanismes de sécurité/chiffrement suivants sont utilisés :

- Solution d'accès ⟷ Cloud (LEGIC Trusted Service) :
  Communication chiffrée : HTTPS over TLS
- Cloud (LEGIC Trusted Service) ⟷ Smartphone :
  communication chiffrée : HTTPS over TLS, certificate pinning
- Composant de porte – Smartphone :
  Mutual Authentication avec les clés de session AES128, de nouvelles clés de session pour chaque session

Le chiffrement des clés digitales pour la commande des accès est effectué en tant que chiffrement End2End à partir du cloud (LEGIC Trusted Service) vers le composant de porte. Un module de sécurité matériel (HSM) est utilisé dans le cloud (LEGIC Trusted Service) au sein d'un environnement de sécurité certifié de la plate-forme LEGIC pour générer les clés de chiffrement/déchiffrement.

Quelles données sont transmises via les interfaces ?

Les données d'autorisation (clés digitales) sont transmises uniquement sous forme chiffrée entre le cloud (LEGIC Trusted Service) et le composant de porte (puce LEGIC) et ne sont stockées sur le smartphone que sous forme chiffrée. Pour la sélection du fichier sur le smartphone, d'autres identifiants sont transmis avec le fichier.
La clé digitale contient des données sensibles, qui sont chiffrées End2End comme décrit dans les chapitres précédents. En outre, il existe encore d'autres données non sensibles qui ne sont pas transmises sous forme chiffrée End2End mais qui sont chiffrées sur les interfaces respectives.
Les données suivantes sont transmises sur les interfaces indiquées ci-dessous :

Interface : Solution d'accès ⟷ Cloud (LEGIC Trusted Service)

- Informations sur les clés digitales (Infini-ID ou Infinilink)
- Informations supplémentaires sur les clés digitales qui sont affichées sur le smartphone, appelées métadonnées LEGIC (par ex., nom de la clé digitale [pour Infini-ID] ou de la personne [pour Infinilink], temps d'attribution de la clé digitale, durée de validité de la clé digitale [Infinilink], nom de l'entreprise)
- Messages d'accès via l'interface smartphone :
  Cloud (LEGIC Trusted Service) ⟷ Smartphone :
- Clés digitales (Infini-ID ou Infinilink) – chiffrées End2End
- Informations supplémentaires sur les clés digitales qui sont affichées sur le smartphone, appelées métadonnées LEGIC
- Messages d'accès via smartphone

Interface : Smartphone – Composant de porte :

- Clés digitales (Infini-ID ou Infinilink) – chiffrée End2End
- Informations de commande pour le processus (accès avec ou sans interaction de l'utilisateur sur le smartphone, ...)
- Informations d'état du composant de porte, qui sont affichées dans l'application (accès autorisé, accès refusé, ...)
- Messages d'accès via smartphone

Qui établit la connexion ?

La connexion entre le smartphone et le cloud (LEGIC Trusted Service) est établie à partir du smartphone afin, par exemple, de consulter les données mises à disposition.
La connexion entre le smartphone et le composant de porte est initiée et contrôlée par le composant de porte.

Comment la connexion est-elle sécurisée ?

La sécurisation de la transmission et des connexions se fait de plusieurs manières :

1. Les données sensibles (clés digitales) sont chiffrées End2End, c'est-à-dire que sur la voie de transmission entre le cloud (LEGIC Trusted Service) et le composant de porte (puce LEGIC), ces données sont chiffrées en permanence et il n'y a aucun matériel clé sur les composants de transmission (notamment l'application « dormakaba mobile access » sur smartphones) pour lire, écrire ou modifier ces données sensibles. Le matériel clé pour le chiffrement et le déchiffrement est disponible exclusivement dans le cloud (LEGIC Trusted Service) et le composant de porte (puce LEGIC) (voir également la section Chiffrement End2End).
2. En plus du chiffrement End2End, toutes les interfaces de communication sont sécurisées/ chiffrées. D'une part, cela protège la transmission de données moins sensibles ; d'autre part, cela offre une protection contre divers scénarios d'attaque.
   - Pour la sécurisation/le chiffrement de toutes les interfaces de communication, reportez-vous à la section Quels sont les chiffrements utilisés entre les différents composants ?
   - Pour vous protéger contre les scénarios d'attaque, reportez-vous à la section Puis-je pirater une clé digitale et obtenir un accès non autorisé ?

La connexion est-elle chiffrée End2End ?

Lors de la connexion du cloud (LEGIC Trusted Service) au composant de porte (puce LEGIC), les données sensibles (clés digitales) sont chiffrées End2End (voir aussi les sections Chiffrement End2End et Comment la connexion est-elle sécurisée ?).
La raison principale du chiffrement End2End est que les informations sensibles sont chiffrées sur le smartphone. Les clés de déchiffrement ne sont pas présentes sur le smartphone, ainsi les informations (clés digitales) ne peuvent être ni lues, ni évaluées, ni modifiées.

Comment les clés de chiffrement/ déchiffrement sont-elles transférées aux composants de porte ?

Le matériel clé pour le déchiffrement (éventuellement aussi pour le chiffrement) est également chiffré à partir du cloud (LEGIC Trusted Service) vers le composant de porte (puce LEGIC) et de plus sécurisé et transmis sur un second canal. Voir aussi la section Clé de chiffrement/déchiffrement.

Comment les clés sont-elles stockées sur le smartphone ?

Il faut distinguer deux types de clés :
- Clés digitales
- Clé de chiffrement/déchiffrement

Clés digitales
Les clés digitales sont stockées au sein de l'application dans une base de données chiffrée.
Les clés digitales sont également chiffrées différemment pour chaque application installée (c'est-à-dire pour chaque instance respective de l'application). Même s'il était possible de copier une telle clé digitale, ceci empêcherait qu'elle puisse être utilisée sur un autre smartphone.

Clé de chiffrement/déchiffrement
Les clés utilisées pour chiffrer ou déchiffrer les clés digitales ne sont jamais transférées sur le smartphone et ne sont donc jamais stockées sur ce dernier.
Le smartphone n'utilise que du matériel clé dérivé pour sécuriser la connexion de communication (NFC/Bluetooth®) avec le composant de porte. Ces clés dérivées sont actuellement stockées sous forme chiffrée sur iOS dans le Key Store sous Android.

La communication entre le smartphone et le composant de porte est-elle plus sûre via NFC ou Bluetooth® ?

En général, l'établissement de la connexion et la sécurisation des deux canaux de communication NFC et Bluetooth® sont identiques, bien que NFC ne parcoure que de courtes distances et que la connexion NFC soit donc plus difficile à intercepter que la connexion Bluetooth®. Dans les deux cas Mutual Authentication, de nouvelles clés de session pour chaque session sont utilisées dès qu'un accès à une clé digitale a lieu (LEGIC neon File). La connexion est donc sécurisée et seules des données sécurisées sont transmises, qui sont évaluées pour l'octroi de l'accès.
En plus des clés digitales (LEGIC neon File), d'autres données non sensibles qui ne sont pas protégées par les mécanismes mentionnés ci-dessus sont échangées par messagerie. Ces données non sensibles sont utilisées pour permettre, par exemple, des fonctions confort. Également pour ces données, Mutual Authentication, de nouvelles clés pour chaque session, est utilisée sur les canaux de communication NFC et Bluetooth®. Un exemple étant les informations d'état du composant de porte, qui sont affichées dans l'application (accès autorisé, accès refusé, ...).

La communication entre le smartphone et le composant de porte peut-elle être interceptée ?

Dès que le composant de porte a établi et sécurisé une connexion pour la lecture des clés digitales à partir du smartphone, l'ensemble de la communication est sécurisé par des clés de session individuelles. L'interception de la connexion ne fournit aucune information sur le contenu chiffré transmis et ne peut pas être utilisée pour des attaques par rejeu.

Puis-je pirater une clé digitale et obtenir un accès non autorisé ?

De manière systématique, un certain nombre de mécanismes de sécurité cryptographiques empêchant une telle manipulation sont utilisés pour la sécurisation des clés digitales. Cela empêche le piratage d'une clé digitale (c'est-à-dire le déchiffrement et/ou la modification du contenu).
Le principe de base est le chiffrement End2End des clés digitales (du cloud au composant de porte) et, en particulier, aucune clé n'est disponible dans l'appli dormakaba mobile access sur le smartphone pour chiffrer ou déchiffrer les clés digitales, de sorte que ni les clés digitales ne peuvent être modifiées (piratées) sur le smartphone, ni sur les voies de communication du cloud vers le smartphone ou du smartphone vers le composant de porte. Toutefois, cela n'exclut pas à 100 % tous les vecteurs d'attaque, tels que la copie d'une clé digitale, si un attaquant a déjà accès au smartphone (smartphone rooté/débridé), les clés digitales étant néanmoins toujours soumises au chiffrement End2End.
La solution Mobile Access repose donc sur des principes garantissant que chaque clé est unique afin d'éviter les attaques systémiques (scénarios de piratage tels que : « Attaque de l'homme du milieu », « Adversary Issuer Attack », « Attaque par rejeu » et « Attaque par relais »).

Comment se protéger contre des scénarios d'« attaque de l'homme du milieu » ?

Pour se protéger contre les scénarios d'« attaque de l'homme du milieu », la protection est assurée sur les interfaces suivantes, comme indiqué ci-dessous :

- Solution d'accès ⟷ Cloud (LEGIC Trusted Service) :
- Communication chiffrée : HTTPS over TLS
- Cloud (LEGIC Trusted Service) ⟷ Smartphone :
- Communication chiffrée : HTTPS over TLS, certificate pinning
- Composant de porte – Smartphone : Mutual Authentication avec les clés de session AES128, de nouvelles clés de session pour chaque session

Comment se protéger contre les scénarios d'attaque « Adversary Issuer » ?

Utilisation du chiffrement End2End, c'est-à-dire en particulier pas d'accès aux données sensibles (clés digitales) sur le smartphone :

- Chiffrement des données sensibles (clés digitales) dans le cloud (LEGIC Trusted Service)
  Pas de clés sur le smartphone pour lire/modifier/écrire des données sensibles (clés digitales)
- Déchiffrement (temporaire) des données sensibles (clés digitales) dans le composant de porte pour la décision d'accès

Comment se protéger contre les scénarios d'attaque « par rejeu » ?

Dès que le composant de porte est authentifié pour la lecture des autorisations d'accès (clés digitales) par le smartphone, l'ensemble de la communication est sécurisé par des clés de session individuelles. L'interception de la connexion ne fournit ainsi aucune information sur le contenu chiffré transmis et ne peut donc pas être utilisée pour des attaques par rejeu.

Comment se protéger contre les scénarios d'attaque « par relais » ?

Pour assurer la protection contre les attaques par relais, les clés digitales du smartphone ne sont qu'activées explicitement pour une courte durée, puis de nouveau désactivées. Lorsqu'elles sont désactivées, les clés digitales ne sont pas lisibles et ne peuvent donc pas être utilisées pour une attaque par relais. L'activation est une action explicite devant être effectuée par l'utilisateur sur l'application (activation par bouton). Après une communication réussie avec le composant de porte et la décision d'accès par le composant de porte, les clés digitales sont directement désactivées. Si aucune communication avec un périphérique n'a eu lieu, les fichiers sont désactivés au bout d'un délai prédéfini.
Dans le cas d'un accès avec un smartphone sans intervention de l'utilisateur, les clés digitales ne sont pas explicitement activées par l'utilisateur, de sorte que dans ce cas il n'y a pas de protection contre une attaque par relais. Pour cette raison, il est recommandé d'utiliser le scénario Accès avec smartphone sans interaction de l'utilisateur comme fonction confort uniquement dans la zone protégée (par ex., portes de bureau dans une zone sécurisée) et d'utiliser le scénario Accès avec smartphone avec interaction utilisateur pour accéder à une zone non protégée (par ex., porte d'entrée).

Mon smartphone peut-il être cloné ?

Il n'existe actuellement aucune protection cryptographique contre le clonage d'un smartphone. Une condition préalable à une telle protection serait la prise en compte d'une fonctionnalité matérielle sécurisée/non modifiable de chaque SmartDevice, qui n'existe pas actuellement.
La protection contre le clonage du smartphone s'effectue exclusivement au niveau de l'application :

- Les clés Infinilink ont une validité limitée,
  après expiration de la validité aucun accès n'est possible. La période de validité détermine donc la période de vulnérabilité possible.
  la validité peut être configurée dans la solution d'accès supérieure ; plus la période de validité est courte, plus la clé Infinilink expire rapidement et l'accès n'est plus possible

Un smartphone perdu/volé peut-il encore être utilisé pour Mobile Access ?

Pour protéger le smartphone contre toute utilisation non autorisée, les mécanismes de protection du smartphone doivent être utilisés. De telles mécanismes de protection du smartphone sont, par exemple :

- PIN
- Empreinte digitale
- Reconnaissance faciale

Ces mécanismes de protection protègent déjà le smartphone contre une utilisation non autorisée au niveau du système d'exploitation. À cette fin, l'exploitant doit prendre les mesures ou appliquer les consignes techniques ou organisationnelles appropriées.

En outre, les possibilités suivantes existent pour empêcher l'accès grâce à un smartphone perdu ou volé si les mécanismes de protection du smartphone ont été rompus :

- Révocation des droits d'accès et donc des clés digitales du smartphone (via les canaux de communication existants du cloud vers le smartphone)
  – La révocation des clés digitales du smartphone s'effectue à partir de la solution d'accès supérieure, qui rappelle les clés digitales via le cloud (LEGIC Trusted Service) et les retire ainsi du smartphone.
  – La révocation est réussie si le smartphone est accessible (par ex., WLAN/Wi-Fi ou communication mobile)
- FSi le smartphone n'est pas accessible (par ex., aucune communication WLAN/Wi-Fi ou communication mobile ou communication du smartphone explicitement désactivée : Mode avion) :
  – Infinilink : L›application vérifie si le smartphone dispose d›une connexion Internet fonctionnelle. Si ce n›est pas le cas pendant plus de 24 heures, l›utilisateur du smartphone reçoit un message d›avertissement correspondant et peut, le cas échéant, réagir (désactiver le mode avion ou activer les données mobiles ou la connexion WIFI). S›il n›y a pas de connexion Internet pendant plus de 30 heures, les droits d›accès existants sont désactivés sur le smartphone, l›utilisateur du smartphone en est informé et est invité à se connecter à Internet. Une fois la connexion à Internet établie avec succès, les droits d›accès présents sur le smartphone sont mis à jour et l›accès est à nouveau possible - conformément aux droits d›accès actuels.
  – Infinilink/Infini-ID : Entrée dans la liste noire des composants de porte (via une solution d'accès supérieure)

Quel est le niveau de sécurité du cloud LEGIC ?

L'accès au service cloud (LEGIC Trusted Service) est soumis à la gestion des autorisations.
Toutes les instances des solutions d'accès utilisant le service cloud (LEGIC Trusted Service) ont une clé API individuelle.
La communication est sécurisée via https/TLS. Les accès individuels au service de cloud (LEGIC Trusted Service) séparent les différentes instances les unes des autres.
Il y a des règles d'organisation pour l'accès au service cloud (LEGIC Trusted Service) par dormakaba à des fins de service.

Quelles sont les recommandations en matière de sécurité pour l'utilisation de lecteurs en ligne, de composants sans fil (wireless) et standalone ?

Pour l'utilisation de lecteurs en ligne et de composants sans fil, le modèle d'autorisation avec Infini-ID est recommandé car les autorisations peuvent être directement mises à jour sur ces composants de porte (en raison de connexions online ou wireless existantes).
Le modèle d'autorisation avec Infinilink est recommandé pour l'utilisation de composants standalone, car les personnes sont en possession des autorisations et aucune mise à jour manuelle des composants standalone n'est nécessaire en cas de modification des autorisations.
En cas de suspicion d'attaque :

- pour les composants standalone,
  - e smartphone doit être accessible pour supprimer Infinilink ou
  - une distribution manuelle d'une entrée dans la liste noire sera nécessaire ou
  - il serait possible d'accéder au composant de porte jusqu'à l'expiration de la validité d'Infinilink.
- pour les lecteurs en ligne et les composants sans fil
  - Les autorisations peuvent être immédiatement révoquées, bloquées ou mises sur liste noire sans distribution manuelle.
  - L'accès peut ainsi être directement empêché.

Du point de vue de la sécurité, l'utilisation de lecteurs en ligne et de composants sans fil est donc préférable.

Quelles sont les recommandations pour l'utilisation dans différents domaines de lecteurs en ligne, de composants sans fil et standalone ?

Lors de l'utilisation de lecteurs en ligne et de composants sans fil (wireless, avec Infini-ID), il est possible de retirer immédiatement les autorisations d'accès via des connexions online ou wireless existantes en cas de suspicion d'attaque.
Lorsque vous utilisez des composants standalone (avec Infinilink), il existe différentes manières de bloquer l'accès en cas de suspicion d'attaque, mais elles sont moins pratiques ou peuvent être bloquées par l'attaquant.
Il en résulte la recommandation suivante visant à combiner les aspects de sécurité et de confort :

- Utilisation de lecteurs en ligne et de composants sans fil (avec Infini-ID) sur des portes accessibles depuis des zones publiques (surface extérieure) ; ainsi, l'accent est mis sur l'aspect sécurité
- Utilisation de composants standalone (avec Infinilink) sur des portes qui ne sont pas situées dans l'espace public, c'est-à-dire pour lesquelles l'accès a déjà été accordé, et qui sont sécurisés avec des lecteurs en ligne et des composants sans fil (avec Infini-ID) ; ainsi, l'accent est mis sur l'aspect confort

Cette procédure peut neutraliser une attaque externe potentielle. Pour les portes intérieures, des composants standalone dotés d'autres caractéristiques confort peuvent être utilisés si une évaluation des risques le permet.

Informations supplémentaires

Définition	Description
Composant de porte	Terme générique pour les lecteurs en ligne, composants standalone ou sans fil (wireless) qui sont utilisés pour Mobile Access.
Solution d'accès	Application de commande/de niveau supérieur (logiciel) gérant les autorisations d'accès, contrôlant la transmission des informations de configuration nécessaires au composant de porte et la distribution des clés digitales.
NFC	Near Field Communication Une norme de transmission pour la communication sans fil d'une portée de quelques centimètres.
BLE	Bluetooth® Low Energy Une technologie radio à faible consommation d'énergie avec laquelle les appareils peuvent être mis en réseau dans un environnement pouvant s'étendre jusqu'à 10 mètres. Bluetooth® est une marque déposée de Bluetooth SIC Inc.
Clés digitales	Informations spécifiques à l'utilisateur sur le smartphone qui permettent au composant de porte de prendre des décisions d'accès.
Infini-ID	Clé digitale : Comprend un numéro identifiant le smartphone/la personne, qui est évalué pour les décisions d'accès par le composant de porte. L'évaluation dans le composant de porte a lieu pour comparer un ensemble d'identifiants Infini-ID enregistrés dans le composant de porte, éventuellement avec d'autres règles d'accès.
Infinilink	Clé digitale : Comprend les règles d'accès d'une personne pour exactement un composant de porte. Ce droit d'accès est valable pour une durée limitée et doit être renouvelé régulièrement (de manière automatique) pour permettre l'accès au composant de porte. Le smartphone doit être accessible pour la mise à jour. Aucun accès n'est possible après expiration de l'intervalle de validité.
Liste noire	Quantité d'identifiants Infini-ID enregistrés dans un composant de porte et empêchant l'accès des personnes portant ces numéros (Infini-ID) à ce composant de porte. En saisissant un numéro de personne/smartphone (Infini-ID) dans la liste noire, l'accès peut être empêché, même s'il existe d'autres autorisations d'accès.
Clé de chiffrement/déchiffrement	Clés cryptographiques pour le chiffrement et le déchiffrement d'informations (par ex., des clés digitales)

Définition	Description
Clés aléatoires	Clés de chiffrement/déchiffrement générées de manière aléatoire dans le HSM (Hardware Security Module), explicitement aucune clé générée manuellement (keys randomly generated in hardware security modules (HSM))
HSM	Hardware Security Module
Le scénario d'« attaque de l'homme du milieu »	Est une forme d'attaque qui trouve son application dans les réseaux informatiques. L'attaquant se tient soit physiquement, soit – aujourd'hui le plus souvent – logiquement entre les deux partenaires de communication, contrôle totalement le trafic de données entre deux ou plusieurs participants du réseau grâce à son système et peut visualiser et même manipuler les informations à volonté. La duplicité de l'attaquant consiste dans le fait qu'il prétend être l'interlocuteur respectif des partenaires de communication. (https://fr.wikipedia.org/wiki/Attaque_de_l%27homme_du_milieu)
Scénario d'attaque « par rejeu »	Une attaque par rejeu (attaque par réinjection) est une attaque cryptoanalytique par rapport à l'authenticité des données dans un protocole de communication. Dans ce cas, l'attaquant envoie des données préenregistrées afin de simuler une autre identité que la sienne. (https://fr.wikipedia.org/wiki/Attaque_par_rejeu)
Smartphone rooté	Le rootage d'un appareil avec un système d'exploitation basé sur Linux, en particulier les smartphones et les tablettes fonctionnant sous le système d'exploitation Android, signifie que des droits étendus sont conférés pour et par l'utilisateur. Ces droits sont également appelés droits root ou droits d'administrateur. (https://fr.wikipedia.org/wiki/Root_d%27Android)
Débridage (iOS)	Signifie la suppression non autorisée de restrictions d'utilisation sur les ordinateurs dont les fabricants ont désactivé certaines fonctionnalités en standard. (https://fr.wikipedia.org/wiki/Jailbreak_d%27iOS)
IT Security Manager	L'Information Security Manager è responsabile affinché tutti i beni, le informazioni, i dati e i servizi informatici di un'azienda siano sempre protetti dal punto di vista della loro riservatezza, integrità e disponibilità. Questa figura è normalmente integrata nella gestione della sicurezza di tutta l'azienda.

Des questions ?

Nous vous conseillons volontiers.

Visitez :

Mobile Access Webpage
by dormakaba

Sous réserve de modifications sans notification.
© 2023 dormakaba. Version 01/2023.

dormakaba
Belgium N.V.
Monnikenwerve 17-19
BE-8000 Brugge
T +32 50 45 15 70
info.be@dormakaba.com
dormakaba.be

dormakaba
France S.A.S.
2-4 rue des Sarrazins
FR-94046 Créteil cedex
T +33 1 41 94 24 00
marketing.fr@dormakaba.com
dormakaba.fr

dormakaba
Luxembourg SA
Duchscherstrooss 50
LU-6868 Wecker
T +352 26710870
info.lu@dormakaba.com
dormakaba.lu

dormakaba
Suisse SA
Chemin de Budron A5
CH-1052 Le Mont-sur-Lausanne
T +41 848 85 86 87
info.ch@dormakaba.com
dormakaba.ch