Giesecke+Devrient
Creating Confidence

StarSign® Key Fob

Data protection information

Giesecke+Devrient

April 2021

www.gi-de.com

Data protection information for the StarSign® Key Fob app

The StarSign® Key Fob app (hereinafter “App”) is used to register and manage fingerprints and FIDO keys on the Key Fob, a device with a fingerprint sensor used for the authentication of individuals by means of the FIDO® protocol from FIDO® Alliance. To this end, an encrypted electronic template is generated using the fingerprint’s individual features and is stored on the Key Fob. The template cannot be viewed by us or other third parties at any time. The template is also not transferred.

In order to enable management in the app, individual IDs are assigned to the templates stored on the Key Fob, and these are displayed in the App. Individual naming via a free text field enables templates to be individually assigned or deleted. Equally, FIDO keys stored on the Key Fob can be managed and assigned using the App.

Depending on the system used (Android/iOS), the following authorizations are needed for use of the App:

- BLUETOOTH: Use of Bluetooth (Android/iOS)
- ACCESS_FINE_LOCATION: Use of Bluetooth (Android)
- ACCESS_BACKGROUND_LOCATION: Use of Bluetooth (Android)

The authorizations are used exclusively for the provision of App functions. No usage beyond this takes place.

The duration of storage for the data in the App and respectively on the mobile end device, as well as on the Key Fob, is managed exclusively by the user. The data are physically deleted as soon as deletion is triggered via management of the templates and FIDO keys, or if a factory reset is performed in the App. Details of how to do this are available in the user handbook.

We reserve the right to amend or update this data protection information to adapt it to the App’s functions and procedures.

Datenschutzhinweise für die StarSign® Key Fob App

Die StarSign® Key Fob App (nachfolgend „App“) dient der Registrierung und Verwaltung von Fingerabdrücken und FIDO Schlüsseln auf dem Key Fob, einem Gerät mit Fingerabdrucksensor zur Authentifizierung von Personen mittels dem FIDO®Protokoll der FIDO®Alliance. Dazu wird auf dem Key Fob anhand der individuellen Merkmale des Fingerabdrucks ein verschlüsseltes elektronisches Muster (Template) generiert und gespeichert. Das Muster kann zu keinem Zeitpunkt von uns oder anderen Dritten eingesehen werden. Auch eine Übertragung des Musters findet nicht statt.

Um die Verwaltung in der App zu ermöglichen, werden den auf dem Key Fob gespeicherten Mustern individuelle IDs zugeordnet, die in der App dargestellt werden. Durch eine individuelle Benennung mittels Freitextfeld können Muster individuell zugeordnet oder wieder gelöscht werden. Gleichermaßen können auf dem Key Fob gespeicherte FIDO Schlüssel über die App verwaltet und zugeordnet werden.

In Abhängigkeit des verwendeten Systems (Android/iOS) werden für die Nutzung der App folgende Berechtigungen benötigt:

- BLUETOOTH: Verwendung von Bluetooth (Android/iOS)
- ACCESS_FINE_LOCATION: Verwendung von Bluetooth (Android)
- ACCESS_BACKGROUND_LOCATION: Verwendung von Bluetooth (Android)

Die Berechtigungen werden ausschließlich für die Bereitstellung der App-Funktionen verwendet. Eine weitergehende Verwendung findet nicht statt.

Die Speicherdauer der Daten in der App bzw. auf dem mobilen Endgerät sowie auf dem Key Fob wird ausschließlich vom Benutzer gesteuert. Die Daten werden physikalisch gelöscht, sobald die Löschung über die Verwaltung der Muster und FIDO Schlüssel veranlasst oder ein sog. Factory Reset über die App durchgeführt wird. Einzelheiten dazu finden sich im Benutzerhandbuch.

Wir behalten uns vor, diese Datenschutzhinweise zu ändern oder zu aktualisieren, um sie an die Funktionen und Verfahren der App anzupassen.

Declaración relativa a la protección de datos de la app StarSign® Key Fob

La app StarSign® Key Fob (en lo sucesivo, «app») sirve para registrar y administrar huellas dactilares y claves FIDO en el Key Fob, un dispositivo con sensor de huellas dactilares para la autenticación de personas basado en el estándar FIDO® de la FIDO® Alliance. Para ello, se genera y almacena en el Key Fob un patrón (plantilla) electrónico cifrado basado en las características individuales de la huella dactilar. El patrón no puede ser visto por nosotros ni por terceros en ningún momento ni se transfiere.

Para permitir la administración en la app, los patrones almacenados en el Key Fob tienen asignados ID individuales que se muestran en la app. Cada patrón dispone de un campo de texto libre que permite asignarle un nombre o borrarlo. Asimismo, las claves FIDO almacenadas en el Key Fob se pueden administrar y asignar a través de la app.

Dependiendo del sistema utilizado (Android o iOS), se requieren las siguientes autorizaciones para utilizar la app:

- BLUETOOTH: uso de Bluetooth (Android/iOS)
- ACCESS_FINE_LOCATION: uso de Bluetooth (Android)
- ACCESS_BACKGROUND_LOCATION: uso de Bluetooth (Android)

Las autorizaciones se utilizan exclusivamente para facilitar las funciones de la app. No se utilizan para ninguna otra cosa.

Es exclusivamente el usuario quien controla el periodo de conservación de los datos en la app o en el dispositivo móvil, así como en el Key Fob. Los datos se eliminan físicamente en cuanto se inicia la eliminación a través de la administración de los patrones y las claves FIDO o se realiza un restablecimiento a los valores de fábrica a través de la app. El manual del usuario contiene todos los detalles al respecto.

Nos reservamos el derecho a cambiar o actualizar esta declaración relativa a la protección de datos para adaptarla a las funciones y los procedimientos de la app.

Déclaration relative à la protection des données pour l'application StarSign® Key Fob

L'application StarSign® Key Fob (appelée ci-dessous « application ») sert à enregistrer et gérer des empreintes digitales et des clés FIDO sur le Key Fob, un appareil équipé d'un capteur d'empreintes digitales pour l'authentification des personnes à l'aide du protocole FIDO®Protokoll de la FIDO®Alliance. À cette fin, un motif (template) électronique crypté est généré à partir des caractéristiques individuelles de l'empreinte digitale et enregistré sur le Key Fob. Ce motif ne peut à aucun moment être visualisé par nous ou par d'autres tiers. Il n'est transmis à aucune personne ou organisme.

À des fins de gestion, un ID individuel est attribué aux motifs enregistrés sur le Key Fob, accessible dans l'application. Les motifs peuvent être affectés individuellement ou supprimés grâce à un nom individuel saisi dans un champ de texte libre. De la même manière, les clés FIDO enregistrées sur le Key Fob peuvent être gérées et affectées à l'aide de l'application.

En fonction du système utilisé (Android/iOS), l'utilisation de l'application requiert les autorisations suivantes :

- BLUETOOTH : utilisation du Bluetooth (Android/iOS)
- ACCESS_FINE_LOCATION : utilisation du Bluetooth (Android)
- ACCESS_BACKGROUND_LOCATION : utilisation du Bluetooth (Android)

Ces autorisations sont utilisées exclusivement pour la mise à disposition des fonctionnalités de l'application. Elles ne sont employées à aucune autre fin.

L'utilisateur est le seul à pouvoir gérer la durée de conservation de ses données dans l'application, sur son appareil mobile et sur le Key Fob. Les données sont physiquement supprimées dès que leur suppression est initiée via la gestion des motifs et des clés FIDO ou lorsqu'une Factory Reset est effectuée via l'application. Vous trouverez plus de détails à ce sujet dans le manuel de l'utilisateur.

Nous nous réservons le droit de modifier ou d'actualiser la présente déclaration pour l'adapter aux fonctionnalités et procédures de l'application.

Informativa sulla protezione dei dati per l'app StarSign® Key Fob

L'app StarSign® Key Fob (di seguito "App") è utilizzata per la registrazione e la gestione di impronte digitali e chiavi FIDO sul Key Fob, un dispositivo con un sensore di impronte digitali per l'autenticazione di persone mediante il protocollo FIDO® della FIDO®Alliance. A tale scopo, un modello elettronico criptato (template) viene generato e memorizzato sul Key Fob sulla base delle caratteristiche individuali dell'impronta digitale. In nessun caso il modello può essere visualizzato da noi o da altri soggetti terzi. Anche la sua trasmissione non ha luogo.

Per consentire la gestione all'interno dell'app, ai modelli memorizzati sul Key Fob vengono assegnati ID individuali, visualizzati nell'app. Nominandoli singolarmente mediante un campo di testo libero, è possibile assegnare in modo individuale o cancellare di nuovo i modelli. Allo stesso modo, le chiavi FIDO memorizzate sul Key Fob possono essere gestite e assegnate tramite l'app.

A seconda del sistema utilizzato (Android/iOS), sono necessarie le autorizzazioni seguenti per usare l'app:

- BLUETOOTH: Utilizzo del Bluetooth (Android/iOS)
- ACCESS_FINE_LOCATION: Utilizzo del Bluetooth (Android)
- ACCESS_BACKGROUND_LOCATION: Utilizzo del Bluetooth (Android)

Le autorizzazioni sono impiegate esclusivamente per la fornitura delle funzioni dell'app. Un ulteriore utilizzo non ha luogo.

Il periodo di memorizzazione dei dati nell'app o sul dispositivo mobile e sul Key Fob è controllato soltanto dall'utente. I dati vengono fisicamente cancellati non appena la cancellazione viene avviata tramite la gestione dei modelli e delle chiavi FIDO oppure viene eseguito un cosiddetto Factory Reset dall'app. I dettagli sono riportati nel manuale utente.

Ci riserviamo il diritto di modificare o aggiornare la presente informativa sulla protezione dei dati, al fine di adattarla alle funzioni e alle procedure dell'app.

Política de Privacidade para o aplicativo StarSign® Key Fob

O aplicativo StarSign® Key Fob (doravante “aplicativo”) serve para o registro e gerenciamento de impressões digitais e chaves FIDO no Key Fob, um aparelho com sensor de impressões digitais para autenticação de pessoas através do protocolo FIDO® da FIDO®Alliance. Para isso, com base nas características individuais da impressão digital, um modelo (template) eletrônico criptografado é gerado e armazenado no Key Fob. O modelo não pode ser visualizado por nós nem por terceiros, em nenhum momento. Também não ocorre nenhuma transmissão do modelo.

Para possibilitar o gerenciamento no aplicativo, são atribuídas IDs individuais aos modelos armazenados no Key Fob, que são exibidas no aplicativo. Através de uma designação individual por meio de campo de texto livre, os modelos podem ser individualmente atribuídos ou novamente excluídos. Da mesma forma, as chaves FIDO armazenadas no Key Fob podem ser gerenciadas e atribuídas através do aplicativo.

Dependendo do sistema utilizado (Android/iOS), são necessárias as seguintes permissões para o uso do aplicativo:

- BLUETOOTH: Utilização de Bluetooth (Android/iOS)
- ACCESS_FINE_LOCATION: Utilização de Bluetooth (Android)
- ACCESS_BACKGROUND_LOCATION: Utilização de Bluetooth (Android)

As permissões são utilizadas exclusivamente para a disponibilização das funções do aplicativo. Não há nenhuma outra utilização além disso.

A duração de armazenamento dos dados no aplicativo ou no dispositivo móvel, bem como no Key Fob, é controlada exclusivamente pelo usuário. Os dados são excluídos fisicamente assim que a exclusão é feita através do gerenciamento dos modelos e chaves FIDO, ou quando é realizado um chamado Factory Reset através do aplicativo. Mais detalhes podem ser encontrados no manual do usuário.

Reservamo-nos o direito de alterar ou atualizar esta Política de Privacidade para adaptá-la às funções e aos processos do aplicativo.

Giesecke+Devrient

About Giesecke+Devrient

Giesecke+Devrient (G+D) is a global security technology group headquartered in Munich. As partner to organizations with highest demands, G+D engineers trust and secures essential values with its solutions. The company's innovative technology protects physical and digital payments, the connectivity of people and machines, the identity of people and objects, as well as digital infrastructures and confidential data.

G+D was founded in 1852. In the fiscal year 2020, the company generated a turnover of 2.31 billion euros with around 11,500 employees. G+D is represented by 74 subsidiaries and joint ventures in 32 countries. Further information: www.gi-de.com.

Giesecke+Devrient

Giesecke+Devrient Mobile Security GmbH
Prinzregentenstrasse 159
81677 Munich
Germany

Phone: +49 89 41 19-0
E-Mail: info@gi-de.com
https://www.gi-de.com

More insights