Privacy Statement for SkIDentity-Service

ecsec GmbH acts as a provider of the SkIDentity-Service and takes the protection of your personal data seriously. The protection of privacy while processing personal data is a very important issue. In particular, personal information will be strictly collected, processed or used in accordance with the legal regulations, especially those of the General Data Protection Regulation (GDPR), the German Data Protection Act (BDSG), the German Act for Telemedia Services (TMG), Act on Identity Cards and Electronic Identification (PAuswG) and the corresponding decree (PAuswV).

Aim of the SkIDentity-Service

The SkIDentity service allows the owner of an electronic identity (eID) card („user“), to get insight into the personal data („attribute“) stored in the respective eID and create a derived electronic identity from this data, which can be stored on the user's system, autonomously managed by the card holder and if necessary used for a completely self-determined identity proofing or a pseudonymous registration at other online services.

Beyond these purposes there will be no other use of the data by the SkIDentity-Service.

Type of the used personal data

The user determines, which identity card is to be used with the SkIDentity-Service. Which attributes are stored on the corresponding card and therefore can be transferred to the derived electronic identity depends on the specific card type. There is an overview of the generally supported credentials and attributes and it is clearly displayed to the user which attributes have been read or will be read from the eID card or the derived electronic identity. Here are some exemplary attributes of the German Identity Card according to § 18 Abs. 3 S. 2 PAuswG listed: family name; birth name; first name; date of birth; location of birth; address; sector-specific pseudonym. The respectively available attributes can at the user´s request be transferred into the derived electronic identity, which can be stored on the user's system. The user can manage the derived electronic identities independently and may manage and delete them. If the user is using the preliminarily created derived electronic identity with other online services for the pseudonymous registration or fully self-determined identity proofing, so-called identity verification tokens are created, with which the authenticity of the identity data can be verified.

Functionality of the SkIDentity-Service

Overview

The SkIDentity-Service is provided under https://skidentity.de and can be reached through clicking on the „ID symbol“. The following functions are available:

- An overview of the available electronic identities
- The creation of new derived electronic identities
- Insight in contents of an electronic identity
- The activation and deactivation of a derived electronic identity
- The protection of a derived electronic identity with a PIN
- The revocation and removal of a derived electronic identity
- The use of derived electronic identities at another online service

Overview of available derived electronic identities

By clicking the „ID symbol“ an overview of the basically on his system available derived electronic identities will be provided to the user. Based on that overview the user can create new derived electronic identities, manage, protect, revoke and finally delete them.

Creation of derived electronic identities

The creation of a derived electronic identity includes the proof of identity of the user against the SkIDentity-Service, the creation of the derived electronic identity by the SkIDentity-Service and finally the storage of the derived electronic identity on the user's local system.

In context of using the German Identity Card (nPA) the SkIDentity-Service acts as a service provider within the meaning of § 2 Abs. 3 PAuswG. Therefore an authorization certificate of the registration authority for access certificates (Vergabestelle für Berechtigungszertifikate, VfB) at the Federal Office of Administration (Bundesverwaltungsamt, BVA) is needed. The authorization certificate allows the SkIDentity-Service to retrieve the authorized data from the German ID card. The communication between the user and the SkIDentity-Service is realized by a web application in conjunction with a suitable eID client according to BSI TR-03124. For data access, the SkIDentity-Service first has to identify itself towards the user. Subsequently the user is able to determine the data that are to be transferred to the derived electronic identity by entering the security PIN.

After the creation of the derived identity by the SkIDentity-Service it will be stored in the user's system and the temporary existing data in the SkIDentity service will be deleted.

Insight in contents of a derived electronic identity

The user can gain insight into the content of a derived electronic identity. This includes the overview of the personal attributes contained in the derived electronic identity and the display of the validity period of the derived electronic identity.

The visualization of the content of a derived electronic identity is performed in the user's local system.

Enabling and disabling a derived electronic identity

Locally stored derived electronic identities can be enabled and disabled by the user. The main difference between an enabled and disabled derived electronic identity is that only an enabled derived electronic identity can be used at another online service.

The activation and deactivation of a derived electronic identity is performed in the user's local system.

Protection of a derived electronic identity with a PIN

For protection against unauthorized access and improper use a locally stored derived electronic identity can be protected by the user with a PIN.

The protection of a derived electronic identity with a PIN, and the removal of the PIN protection respectively, occurs at the user's local system.

Revocation and deletion of a derived electronic identity

The user is able to revoke and irretrievably delete an electronic identity.

Use of a derived electronic identity at another online service

The user is able to use a locally stored and activated derived electronic identity at other online services for a completely self-determined identity proofing or a pseudonymous registration. In this case a copy of the locally stored derived electronic identity is transmitted to the SkIDentity-Service, which can create an identity confirmation token for the respective online service which can be forwarded in a well-informed and self-determined process to the appropriate online service. With the provided identity confirmation token, the authenticity of the identity data can be verified.

All in this way usable online services are outside the scope of responsibility and integrity of the SkIDentity-Service. During the initial connection of an online service to the SkIDentity-Service, it is aligned to § 21 Abs. 2 PAuswG verified, that

- the indicated purpose of the online service shown to the user is applicable and not illegal,
- the purpose of the online service is not to collect and trade identity information for commercial purposes,
- the requested data is required for the specified purpose of the online service,
- the online service has implemented appropriate technical and organizational measures for data protection and
- there is no overall evidence of misuse of the identity data of the user by the online service.

However for this purpose no warranty can be taken over by the SkIDentity-Service. Hence, the user has to independently verify the legality of the online service and the individual compliance with data protection rules.

The SkIDentity-Service does not store the personal data of the user in a permanent manner, it does not pursue transactions with connected on-line services or create user profiles. All data in the SkIDentity-Service will be deleted immediately once they enter the sphere of the user, e.g. the browser. IP addresses are also not stored permanently.

Before using the SkIDentity-Service for the first time, the user explicitly has to confirm the reading of this Privacy Statement and agree with the practices set out in this statement before the first use of SkIDentity-Service.

When using other cards than the German ID card, the basic processes are the same, with the difference, that the SkIDentity-Service does not need an authorization certificate of the registration authority for authorization certificates and the communication may not be handled by an eID client according to BSI TR-03124.

Security

To protect the SkIDentity-Service and therein managed personal data from accidental or intentional manipulation, loss, destruction or against access by unauthorized persons, ecsec GmbH uses state of the art technical and organizational security measures. For example, all communications channels between the system of the user and the SkIDentity-Service are protected with suitable versions of Transport Layer Security (TLS). Furthermore the used security measures are continuously monitored and improved according to the technological development.

Saving data on the user´s local system

The SkIDentity-Service stores the derived electronic identities on the user's local system. By that only the local system users and the SkIDentity-Service can access the data but no other online services. Unless the access to the user´s local system is not controlled otherwise, it is recommended to protect the derived electronic identity with a security PIN.

Protocol data

To maintain the technical operation, the SkIDentity-Service creates various technical log data. In this case no personal data is collected.

Links to other websites

The SkIDentity-Service is available at http://skidentity.com and contains links to other websites. These websites are within the responsibility of the respective website operators. When embedding the external links no legal violations were found. The provider has no influence on the current and future design of the linked page. Without specific evidence of violations the permanent monitoring of the external links is not reasonable for the provider. Upon notification of legal violations, the affected external links will be deleted immediately.

Rights of the concerned person

The user can revoke the agreement concerning the processing of personal data by the SkIDentity-Service, manifested by the issuance of derived electronic identity and storing it in the user's local system, by deleting the derived electronic identity, at any time. The user has the right to obtain information about the type and scope of the stored personal data, the origin of the data and the online services connected to the SkIDentity-Service which may occur within the fully self-determined proof of identity as potential recipients of the data and may request its data in a structured and machine-readable format. This information is available to the user by regular management functions of the SkIDentity-Service or the supplementary website at http://skidentity.com. For further questions the user may use the contact data under the section „Responsible entity“.

Responsible entity

Responsible entity according to Art. 4 Nr. 7 GDPR for the SkIDentity-Service is

ecsec GmbH
Sudetenstrasse 16
96247 Michelau
http://www.ecsec.de

represented by Tina Hühnlein and Dr. Detlef Hühnlein. Further information can be found in the Imprint of ecsec GmbH.

Data Protection Supervisory

The responsible Data Protection Inspectorate according to Art. 51 GDPR for the SkIDentity-Service is the

Landesamt für Datenschutzaufsicht
Promenade 27
91522 Ansbach
http://www.lda.bayern.de/ .