A-Trust GmbH
1030 Wien, Landstraßer Hauptstraße 1b, E02

Information Disclosure in accordance with Article 24 (2) lit d eIDAS Regulation

Information about the terms and conditions for the use of EU-Identity qualified certificates from A-Trust GmbH, Version 2.0

1 Contract components EU-Identity

You enter into an agreement with the qualified trust service provider A-Trust GmbH. A-Trust uses associated registration points for the registration of certificate applicants. The contractual relationship between you and A-Trust consists exclusively of the following contractual documents in their respective valid version:

- the application/signature contract,
- the General Terms and Conditions (GTC) of A-Trust GmbH for qualified and advanced certificates,
- the A-Trust Certificate Practice Statement for qualified certificates EU-Identity,
- the A-Trust Certificate Policy for qualified certificates EU-Identity,
- the A-Trust provisions regarding rates and charges,
- the A-Trust list of recommended components and procedures and
- this information disclosure.

All contract documents have been reviewed and accepted by the governmental supervisory authority and are available for download at www.a-trust.at/downloads. The handling of your personal data is regulated by GDPR, the STA (Signature und Trust Services Act) and the eIDAS Regulation. A-Trust only processes your data as required within its function as trust service provider and insofar as you have given your consent.

In accordance with Article 13 of the eIDAS Regulation, A-Trust is liable for any damages to any natural or legal person, caused intentionally or negligently, resulting from a breach of obligations set forth in this regulation.

2 Signature Contract

With the signature contract, you apply for the issuance of a qualified EU-Identity certificate and define its content. The application of the remaining contract components is agreed upon in the signature contract.

3 Certification Practice Statementand for EU-Identity

The Certification Practice Statement is the generally comprehensible summary of A-Trust's security and certification concept. In the Certification Practice Statement, the technical and organizational requirements for the creation of the qualified certificate by A-Trust, as well as details on registration and activation are revealed to the signatory. In this way everybody, including the potential recipients, respectively verifiers of the signatures, can get an idea of the overall security of EU-Identity.

4 Certificate Policy for EU-Identity

The Certificate Policy specifies the content of the certificate and the requirements for a secure use of the certificate by the signatory. Based on the Certificate Policy, the recipient of a signature can determine whether it is a qualified signature and whether the underlying certificate is a qualified certificate. In addition to the rights and duties of the signatory, the rights and duties of the qualified trust service provider are shown as well. The reliability of a certificate is therefore based on the Certification Policy.

5 Legal effect of electronic signatures

According to Article 25 (2) of the eIDAS Regulation in conjunction with § 4 (1) of the Austrian Signature and Trust Services Act (SVG), the qualified signature has the equivalent legal effect of a handwritten signature. The following exceptions to this principle are standardized in § 4 (2) SVG:

- Testamentary dispositions cannot be effectively established in electronic form.

The following declarations of intent can only be effective in electronic form if the declaration document contains the confirmation of a notary or a lawyer:

- Declaration of intent of family law or inheritance law, which are bound to a written form or a stricter form requirement;
- Guarantee statement (§ 1346 par 2 ABGB (Austrian Civil Code of Law)) issued by persons outside their commercial, business or professional activity.

6 Technical components (signature products), formats and procedures

The components, formats and procedures for qualified signatures recommended by A-Trust are for a quality-assured work environment for the certificate holder, who creates a secure digital signature using a mobile certificate issued by A-Trust. The focus of the recommendation being on the following issues:

- Creation of the qualified signature: You should refrain from using file formats such as dynamic date fields or white-on-white representations as signature formats, in this way, you as well as the receiver can be sure that the document sent by you arrives unaltered.
- Secure verification: A-Trust will provide you with a suitable infrastructure for the verification of a qualified certificate or a signature on the certificate. You can find detailed information on this and the certificate database with the current revocation list for certificate and signature verification on the A-Trust homepage. The use of the functions of the certificate database is free of charge and anonymous.

In case of an error, A-Trust shall only be liable as the provider of trust services insofar as the recommended components, formats and procedures have been used (see https://www.a-trust.at/docs/verfahren).

7 Duties of the signatory

The signatory's handling of the certificate is an essential aspect of the overall security of the qualified signature. The premise of dealing with the signature creation unit and the use of the recommended signature products and procedures are the protection and secrecy of the signature creation data with associated password.

In order to complete a qualified signature, the signature password is mandatory, and the assigned mobile phone number/SIM card has to be solely the signatory's. The assignment of a certificate to a mobile phone number takes place during registration.

The obligations for the signatory arise from the contract documents and from the signature and trust service law. Signatories of EU-Identity certificates must register personally (to define the signature password and assignment of the mobile phone number). The signatories are required to carefully store the signature creation data, to prevent access by third parties, as far as reasonably possible, and to refrain from passing the data on to third parties. Furthermore, the TANs/Verification SMS must be handled carefully. The passing on of electronic signature creation data to authorized persons is permitted. Signatories must request the revocation of the qualified certificate if the electronic creation data is lost, if there are indications of the electronic creation data being compromised, or if the circumstances attested in the qualified certificate have changed.

For your safety, A-Trust recommends:

- to pay attention to the separation of the components and, for example, not to enter the signature password on the same device on which the TAN is received;
- to specify the signature password only on pages where the address line of the browser displays the URL https://www.a- trust.at/ or https://www.handy-signatur.at;
- the verification message containing the TAN contains a comparison value number that is also displayed on the website. It is the signatory's responsibility to verify the match of these two comparison value numbers, ensuring that the correct document is signed;
- all browser functions that save field entries (mobile phone number and signature password) should be deactivated when using the mobile phone signature (e.g. auto-completion, saving of passwords);
- the use of up-to-date security software (virus protection, firewall) to prevent spyware from spying on the signature password;
- do not circumvent the security mechanisms of the operating system of the mobile phone with Roots or Jailbreaks;
- to obtain apps used in connection with the mobile phone signature only from official app stores of the respective providers: Apple App Store, Google Play Store, Windows App Store etc.;
- to have the private key deleted after the revocation of the mobile phone signature certificate. Online implementation, as well as information at https:/www.a-trust.at/widerruf;
- observe the additional information at https://www.a-trust.at/app-security.

8 Revocation service

With the revocation service, A-Trust ensures that revocation or suspension of the certificate is possible at any time, quickly and easily, in the event of concerns about the security of the certificate. This and the possible lifting of a suspension are the only but very important tasks of the revocation service.

The reasons for a revocation can be:

- mobile phone or SIM card was lost, stolen, or is defective,
- you are no longer the sole owner of all SIM cards linked to the mobile phone number,
- certificate data (e.g. your name) has changed.

A-Trust has to suspend a qualified certificate if:

- the signatory or another entitled person so requires,
- the supervisory authority requests the suspension of the certificate,
- A-Trust acquires knowledge of the death of the signatory or changes of the certified certification information,
- the certificate was obtained based on incorrect information, or
- there is a risk of misuse of the certificate.

The lifting of a suspension can take place within the 10-day blocking period, using the revocation password respectively the suspension password, which you receive in the telephonic application for suspension from the revocation service.

The certificate numbers of the revoked or suspended certificates are entered by A-Trust in the Certificate Revocation List (CRL). The CRL, which is signed by A-Trust, is constantly updated so that the status of a certificate can be checked at any time, which is usually done automatically by the software products used.

Further explanations to revocation and suspension, as well as reachability of the revocation service can be found under www.a-trust.at/widerruf.

9 Call Center

If you have technical problems when using EU-Identity or need information about other products or price information, please contact A-Trust's fee-based hotline (1.09 EUR/min; www.a-trust.at/callcenter).

10 Information Disclosure in accordance with eIDAS Regulation: Information about my personal security as a signatory

As a signatory, I confirm with the acknowledgment of the signature contract, that detailed information was made available to me before conclusion of the contract about the following points, and that I accept the same:

A-Trust's services are based on the Certificate Practice Statement (CPS) and the Certificate Policy (CP) for qualified certificats. These documents can be downloaded from the A-Trust homepage and are freely available at the registration office. The maximum validity of my certificate is 5 years. After that, the validity of the certificate must be extended (certificate renewal) or, if necessary, a new certificate must be activated. A-Trust has been accredited by the governmental supervisory authority, the Telecom Control Commission (TCC) and is being reviewed by the TCC accordingly.

A-Trust shall be liable for any intentional or negligent damage incurred to any natural or legal person arising out of a breach of obligation set forth in the eIDAS regulation, the Signature and Trust Services Act or the Signature and Trust Services Regulation. A possible limitation of liability of A-Trust is shown explicitly as transaction limit in the certificate.

The scope of the qualified certificate is not limited. The qualified signature replaces my own handwritten signature. Thus, I can validly submit such statements that require the written form in accordance with the law or an agreement (including general terms and conditions). The exceptions already mentioned in this document comply with the Signature and Trust Services Act (§ 4).

I have to ensure the careful storage of my mobile phone number/SIM card. My mobile phone number/SIM card and the associated signature password can only be accessible to myself and to no one else. I have to choose my password in a way that it cannot be logically derived from my person (e.g. no birthdays). The signature is created through entry of the signature password. To protect my signature password, I need to be aware of which hardware and software I am using and follow the instructions of the manufacturer. A list of recommended hardware and software is available on the A-Trust website.

If the protection of mobile phone number/SIM card or signature password is not guaranteed, I must revoke my certificate at the revocation service of A-Trust. This also applies in the event that the information in the certificate has changed or is incorrect. The revocation of my certificate is made by telephone or by fax by naming my name, the contract number and my chosen revocation password. A-Trust also provides the option of a temporary suspension, which can be reversed by means of the revocation password or an agreed password for lifting the suspension (see www.a-trust-at/widerruf).

The liability of A-Trust for my qualified signature is only guaranteed by using A-Trust recommended technical components and procedures. The A-Trust homepage refers to corresponding products and services for which a secure signature environment can be presumed. Furthermore, I have to take the file formats recommended by A-Trust into account. The recipient of my qualified signature relies on my use of recommended components, as my use of the components is not derivable from the signed electronic content and the signature itself. The recommendations of A-Trust are also available to the recipient in its entirety and in the same form. When using methods and formats other than those recommended by A-Trust, I am obligated to inform the recipient of my signature of the same or enter into a separate agreement with him/her to build a basis of trust for the acceptance of this signature.

Information on the certificate database with the current Certificate Revocation List for certificate validation can be found on the homepage of A-Trust. The use of the certificate database, in accordance with the technical capabilities, is free of charge and anonymous. The same components and procedures are to be used for the signature verification as for the signature creation. I can inform myself on the homepage of A-Trust whether there have been changes regarding the procedures and components I have used. I also have to follow the renewal recommendations of the manufacturers or those of A-Trust.

Some countries limit the import or export of encryption technologies. Before traveling, I have to inform myself about the respective legislation of the respective country. If I am a minor, I have limited contractual capacity. It is therefore mandatory for minors to include the date of birth in the certificate content as a reference for the signature recipient.

11 Disclaimer

The English version of the disclosure is for information purposes only. The terms and conditions set out in the German disclosure shall prevail.