CERTILIA

AKD d.o.o.
web: https://www.certilia.com
email: ra-ured@akd.hr
helpdesk: helpdesk@certilia.com

Application for the Provision of Certification Services

AKD AGENCIJA ZA KOMERCIJALNU DJELATNOST

1. Personal Data on Certification Subject

First Name*

Last Name*

OIB / ID Number*

Identification Document* ☐ ID Card or ☐ Passport   Valid to* | | . | | . | | | | .

Number of Identification Document*

Date of Birth* | | . | | . | | | | .   Sex* ☐ Female   ☐ Male

Residence Address and Contact Info

Street and Number*

Zip Code*   City*

Nationality*

Mobile (SMS)*

E-mail*

2. Service Package

Please select service package (1 to 5). Certificates will be issued on AKD smartcard.
NOTE: This Application includes issuing sms.ID and mobile.ID credentials. Credentials are activated through Portal at https://portal.certilia.com/ free of charge.

Personal Card

☐ **(1) ID Card**
Personal identification certificate (NCP+)

☐ **(2) Signing Card**
Personal signing certificate (QCP)

☐ **(3) ID & Signing card**
Personal signing and identification certificate (QCP & NCP+)

Corporate Card

☐ **(4) Corporate ID Card**
Personal identification certificate (NCP+)

Company Name *

OIB or EU VAT *

☐ **(5) Corporate Signing Card**
Personal signing certificate (QCP)

☐ **(6) Corporate Signing & ID Card**
Personal signing and identification certificate (QCP & NCP+)

3. Statement of the Subject of Certification

Herewith I confirm that all data in this Application are full and accurate. In the case of inconsistency of data indicated in this Application with data acquired from official registers I give permission to AKD to use data acquired from official registers. I confirm that I was informed about statutory requirements for the use of personal data for certification services. I hereby guarantee that only I can access and read electronic messages received at E-mail and SMS messages received on Mobile provided in the point 1 of this Application. By signing this Application I agree with publication of issued certificates pursued AKD's Certification Practice Statement. By signing this Application I agree with Policy disclosure statement (n), enclosed to this document and available at: https://www.certilia.com/dokumenti/.

4. Delivery and Acceptance of the Card and Activation Data

☐ **RA Office**
Card and/or PIN.

☐ **Delivery service**
Proof of identification required. Delivery on address provided in this Application. Separate delivery service for Card/PIN.

☐ **E-mail / SMS**
Activation data – PIN delivered to E-mail/SMS provided in this Application.

5. Signature of Subject of Certification

Date

Signature of Subject of Certification

FILLED BY RA OFFICER

6. Data in case the subject of certification is identified in association with an organizational entity.

Evidence of registration ☐   Type of evidence

Association of natural person with an organizational entity

Signed and verified proof issued by the organization that proves association of natural person with an entity.

Date

Signature of RA officer

RA Office Stamp

* Mandatory data

1. Information about the certification services provider
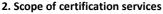
AKD d.o.o, VAT: HR58843087891
Address: Savska cesta 31, 10000 Zagreb, Hrvatska
web: http://www.akd.hr, e-mail: akd@akd.hr
Portal: https://www.certilia.com
EUTL: https://eidas.ec.europa.eu/efda/tl-browser/#/screen/tl/HR
Customer service: helpdesk@certilia.com
Policy management authority: pma@akd.hr.
Personal data protection officer: zastita.podataka@akd.hr.

2. Scope of certification services

Certification services provider provides the following services:

1. certificate generation services
2. certificate revocation services
3. certificate status checking services
4. information services
5. services of card production
6. remote signature and seal creation
7. registration services

3. Types and purpose of the certificate

Certificate generation services includes generation of following certificates:
- kID identification certificate is a means of electronic identification of high security level (OID: 1.3.6.1.4.1.43999.5.5.2.1.2.2),
- kID qualified signing certificate for electronic signature that can legally replace a handwritten signature (OID: 1.3.6.1.4.1.43999.5.4.2.1.2.1) and
- kID qualified signing certificate for remote electronic signature that can legally replace a handwritten signature (OID: 1.3.6.1.4.1.43999.5.4.6.1.2.1) and corresponding private keys.
The validity of the certificates is up to 3 years and up to 2 years for certificates for remote electronic signature. The certificate contains information about the date of expiry and the all data and information necessary to validate the certificate.
There is a natural person named in the certificate as the subject of certification. If sufficient and adequate evidence is provided, there can be a person specified in the certificate named by the organization with whom the natural person is related to. A person that is the subject of certification uses certificates for business and private purposes.
The level of trust in the certificate and the identity of the person named in the certificate is high according to the criteria laid down in EU Regulation no. 910/2014.
kID identification certificate issued according to the rules that are equivalent to the rules of NCP + (OID: 0.4.0.2042.1.2) that apply to normalized certificates with the private key in a secure cryptographic device.
kID qualified signing certificate is issued under the rules of the EU Qualified Certificates QCP-n-qscd (OID: 0.4.0.194112.1.2) to an individual with private key on qualifying device for production of electronic signature.
kID qualified certificate for remote signature is issued under the rules of the EU Qualified Certificates QCP-n-qscd (OID: 0.4.0.194112.1.2) to an individual with signature creation data managed by the qualified trusted service provider on behalf of the individual.

4. Obligations of certification services providers

The certification service provider provides certification services pursuant to (EU) Regulation No. 910/2014 and related legislature and by laws, by applying:
1. provisions of the law governing electronic signature and bylaws adopted under the same law and
2. Internal by laws that regulate provision of certification services
2.1. AKD PKI Certificate policy
2.2. CERTILIA Certification Practice Statement
The certification service provider will:
- Ensure availability of certification service and AKD mPotpis service for remote signature and seal creation,
- Process applications for the issuance, revocation and suspension of certificates on time
- Gather and store all relevant information to the data issued and received, especially for the purpose of presenting evidence in court proceedings and for the purpose of ensuring continuity of service,
- Archive and keep for a period of 10 years after the expiry of the certificate, all the important information that is collected or recorded in the course of provision of certification services,
- Have qualified staff and financial resources sufficient to fulfil its commitments and to ensure continuous provision of services,
- Implement appropriate physical, organizational and enforcement measures for the protection of IS and data,
- Carry out processing and protection of personal data and all other confidential business information in a lawful manner
- publish via https://www.certilia.com web portal all information necessary for the proper use of certification services and cards including this Policy Disclosure Statement and AKD PKI Certificate policy and CERTILIA Certification Practice Statement.

5. The rights and obligations of persons

5.1. Natural person, the subject of certification will:
- Present trustworthy evidence, in the process of identification, to prove his identity and the identity of the organization with which he/she is associated with
- Provide accurate and true information in the registration process
- Examine and verify that the identification information contained in the certificate is accurate,
- Be the only person to use a private key corresponding to the public key in the certificate,
- Make sure that the certificate at the time of its use has not expired and has not been revoked,
- Make sure that the certificate is used only for legal purposes and in accordance with its intended purpose,
- Use the card and PINs responsibly, keep it safe and take all appropriate measures to protect them against unauthorized access and use,
- request revocation or suspension of the certificate immediately if there is a change of identity in the certificate, or if there is a suspicion of loss, theft, misuse or unauthorized use of the card, PIN or the private key.
- Use the certificate in accordance with the provisions of the terms and conditions including but not limited to amendments.
5.2. A person who orders certification services will:
- Report any change of information in their status, name and address, and present accompanying documents.
- Immediately request revocation of the certificate if previously established relations with the person subject of certification terminated or ceased to exist

6. Limitation of liability

The liability of the certification services provider for the damage caused by any natural or legal person due to failure to comply with their obligations is limited to the amount of 265.445,62 EUR. The liability is limited to 10.617,82 EUR per transaction for the people and relying party that use certificates appropriate.

The certification services provider is not liable for:
- Damages caused by improper use of the certificate,
- Damages caused by fraudulent or negligent use of the card, PINs, private keys, certificates and CRL,
- Damages incurred in a period of revocation of certificate until the issuing the new CRL,
- Damages caused by malfunctions and errors of the software and hardware of the natural person and/or their relying party
- All the damages caused intentionally or by negligence of a natural person or relying party that have not met its obligations or fails to act in accordance with their obligations.
The certification services provider is not responsible for damages that are the result of presentation of false information in the registration process or misrepresentation of natural or legal persons in the process of identification and authentication.
The certification services provider is not liable for breaches of liability person and relying parties, especially not for the use of certificates issued by other certification services providers.
The certification services provider is not responsible for the content of the document signed using a private key of a natural person who is the subject of certification, nor for any other form of indirect damage as a result of use of a certificate.

7. Compensation of damages

Any party that caused damages due to breach of law or the provisions of this document is liable to the party suffering damages.
A natural person is liable to party suffering damages if he/she obtains certificate issued by CERTILIA on the basis on false information provided in the application or if he/she operates or presents his or herself on behalf of other natural person.
Relying party is liable to the party suffering damages if they rely on the certificate without checking its validity or if they use certificate for the purposes for which it is not intended or in spite of legal constraints or regulations.
The certification services provider is liable pursuant the terms and regulations of the Agreement, AKD PKI Certificate policy, CERTILIA Certification Practice Statement, this Policy Disclosure Statement and all applicable laws and regulations of the Republic of Croatia.

8. Price

The fee for the issuing of certificate and use of certification services is charged according to the price set by the pricelist or by a contract.

9. Protection of Personal Data

Persons who have been issued a certificate, data subjects, are made aware that the data contained in the certificate are legally protected as personal data, and that certification services provider processes and uses them in their records for the sole purpose of fulfilling the statutory requirements necessary by AKD as controller for implementation of provision of certification services. Personal data are used to meet legal obligations and are kept for a period of 10 years after the expiry of the corresponding certificate. Data subject has the right to request from AKD access, rectification, erasure, portability and restriction of processing of collected data via contact data provided in point 1, provided that the required conditions are fulfilled. Data subject has the right to object to the processing of personal data to the Croatian Personal Data Protection Agency, Selska cesta 136, Zagreb, 00385 (0)1 4609 999, azop@azop.hr. Detailed information can be found in personal data protection statement available on https://www.certilia.com.

10. Protection of confidential business information

The certification services provider protects and handles all information and data collected or incurred during the provision of certification services properly. This applies to the information and data whose disclosure to an unauthorized person could have harmful effects for the services themselves or for the persons, as well as for any data or information marked as confidential or as secret by law on the confidentiality of data or CERTILIA Certification Practice Statement.

11. Conclusion and termination of contract

A person accepts these conditions by signing a request for the provision of certification services. The agreement on the use of certification services is considered concluded at the moment of acceptance of the request filed by natural persons. Disclosure Statement, together with the Application for the provision of certification services or Application for issuing certificate for remote electronic signature and Application for the provision of certification services with organization in subject, make the contract on the provision of certification services.
If a person does not accept this Policy Disclosure Statement, it is not possible to successfully process their request for the issuance of a certificate and issue a certificate.
Revocation of the certificate terminates the agreement and therefore, rights and obligations of all parties established by this Document are thus terminated.

12. Complaints, resolution of disputes and applicable law

The provision and use of certification services is performed in accordance with this Policy Disclosure Statement, AKD PKI Certificate Policy and CERTILIA Certification Practice Statement.
All complaints, disputes and potential disagreements concerning interpretation, application or execution of certification services, will be resolved amicably.
The users of certification services may file a complaint to Customer Service at helpdesk@certilia.com. If the user is not satisfied with such resolution, a complaint may be submitted to the Policy Management Authority pma@akd.hr.
AKD will provide a reply/solution within 15 days from the receipt of such a complaint.
If the dispute is not resolved amicably, then they will be settled before a competent court in Zagreb. The applicable law is the law of the Republic of Croatia.

13. Supervision

AKD is a qualified provider of certification services and its qualified status is indicated on the trusted list.
Supervision of the implementation of Regulation (EU) no. 910/2014 regarding the provisions governing electronic identification is carried out by the central government body in charge of e-Croatia.
Supervision of the implementation of Regulation (EU) no. 910/2014 regarding the provisions governing trust service is carried out by the central government body in charge of commerce and economy.
Performance of audit and verifying compliance with Regulation (EU) no. 910/2014 is carried out by an independent accredited conformity assessment body.
Supervision of processing, use and protection of personal data is carried out by government authorities defined by law and by other directives and regulations that regulate protection of personal data.

14 Final Provisions

In accordance with applicable regulations in Croatia, this Disclosure Statement as well as all other information required for the appropriate use of certification services and of a card are published on the web portal: https://www.certilia.com.
Detailed terms and conditions relating to the use of the certificate are set out in documents AKD PKI Certificate Policy and CERTILIA Certification Practice Statement.