1 Introduction

This publication is intended for service providers wishing to obtain certification of compliance with various regulations/standards/certification schemes. It sets out the conditions for certification and presents the complete process from the application for certification to the issue of a certificate of conformity. The certificate, i.e., the document issued, may also be called something else if the certification scheme provides for a different title for the document granted. This publication also contains information on the maintenance of the certificate and on the revocation or cancellation of the certificate, as well as on confidentiality and complaint handling. The certification of services described in this document is not identical to the certification of management systems.

SIQ Ljubljana (hereinafter SIQ) certifies services as a "third party", i.e., an institution independent of service providers on the one hand, and customers and users on the other. This independence is ensured by its founding status–SIQ is registered as an institute–and by the appropriate organisation of the governance and management of the certification activity. The certification activity is under the supervision of the Board of Certification Body, which represents the interests of public, commercial, and industrial associations and the interests of the customers of the Institute's services.

During the certification process, we assess and evaluate whether a service meets the requirements set for it and, if it does, we issue a certificate of conformity. Decisions on the issue are the responsibility of the Certification Commission for Management Systems.

At SIQ, we provide one type of service certification:

- *Certification of services within a regulated area*.

2 Certification of services within a regulated field

2.1 EIDAS certification

The subject of the certification is a service or group of services for which the client wishes to be certified and can be clearly and unambiguously identified. A certificate may be issued for:

- an electronic signature (issuance, validation, storage);
- an electronic stamp (issuance, validation, storage);
- an electronic time stamp;
- an electronic registered delivery service;
- website authentication.

2.2 Certification criteria

An agreement shall be reached with the applicant on the standards, regulations, or specifications that form the basis for the review and assessment of compliance, e.g., certification of trust services (under Regulation (EU) No 910/2014 - eIDAS):

- Electronic signatures: CP207 (information for applicants), ETSI EN 319 401 v2.3.1, ETSI EN 319 411-1 v1.3.1, ETSI EN 319 411-2 v2.4.1, ETSI EN 319 412-1 V1.4.4, ETSI EN 319 412-2 v2.2.1, ETSI EN 319 412-5 v2.3.1
- Electronic seals: CP207 (subscriber applicants), ETSI EN 319 401 v2.3.1, ETSI EN 319 411-1 v1.3.1, ETSI EN 319 411-2 v2.4.1, ETSI EN 319 412-1 V1.4.4, ETSI EN 319 412-3 v1.2.1, ETSI EN 319 412-5 v2.3.1.
- Electronic time stamps: CP207 (subscriber information), ETSI EN 319 401 v2.3.1, ETSI EN 319 421 v1.1.1, ETSI EN 319 422 v1.1.1.

- Electronic registered delivery service: CP207 (information for applicants), ETSI EN 319 401 v2.3.1, ETSI EN 319 421 v1.1.1, ETSI EN 319 422 v1.1.1
- Website authentication: CP207 (information for applicants), ETSI EN 319 401 v2.3.1, ETSI EN 319 411-1 v1.3.1, ETSI EN 319 411-2 v2.4.1 ETSI EN 319 412-1 v1.4.2, ETSI EN 319 412-4 V1.2.1, ETSI EN 319 412-5 v2.3.1

3 Basic principles of conduct

3.1 Certification policy

SIQ offers certification services to anyone interested.

SIQ, i.e., its bodies and its staff, treats and will treat all subscribers of its services in the same way, regardless of their geographical location, size, turnover, type of business, etc., without disadvantaging anyone in any way.

SIQ maintains an international reputation and recognised status in the field of certification. SIQ strives to ensure that its certificates are increasingly recognised at home and abroad.

SIQ shall ensure independence, impartiality, and an organisational structure such that the staff, in the performance of their day-to-day tasks, are not influenced by anyone with a direct commercial interest in the certification and that there is no conflict of interest in their work. We have mechanisms in place to address potential conflicts.

SIQ performs certification (conformity assessment) in accordance with the requirements of SIST EN ISO/IEC 17065, SIST EN ISO/IEC 17021-x, SIST EN ISO/IEC 17024, SIST TS ISO/TS 22003, ISO 50003, ISO/IEC 27006 and ISO/IEC 20000-6 standards, EMAS Regulation 1221/2009 EC, EIDAS 910/2014 EC, the additional requirements of other directives/regulations/rules of procedure and the applicable related legislation under which it is designated as a Notified Body, SIST EN ISO 14065 with the applicable related legislation and any additional requirements of international schemes.

SIQ carries out its operational activities in accordance with the documented procedures set out in the quality management system documents for each certification area and in accordance with other quality management system documentation.

SIQ charges for its services in accordance with the pricing bases as determined by the SIQ Council. SIQ's service prices cover running costs and investments in the technical and professional development of its activities.

3.2 Rules for certification staff

Certification staff shall work in accordance with the Slovenian, European, and/or international standards, as well as SIQ regulations, procedures, and instructions governing the work in this field. Each member of the staff involved in the certification procedure shall be guided by the following principles and shall undertake to:

- act confidentially and impartially, both in relation to SIQ and in relation to any organisation involved in the certification procedure carried out by him/her or by the personnel for whom he/she is responsible;
- inform SIQ if he/she has any connection with the organisation for which he/she is to carry out the certification procedure, or if he/she has carried out any consultancy work for the services of that organisation in the last two years before taking on any function relating to the certification of the services of that organisation;
- not to accept any inducements, gifts, commissions, discounts, or other benefits from the organisations for which he/she carries out the certification procedure, or from their

representatives, or from any other person who would benefit in any way, and not to allow any of the staff for whom he/she is responsible to do so;
- not to disclose to third parties, either in whole or in part, the results of any certification procedure in which he/she is or has been involved or for which he/she is responsible, nor any information obtained in the course of the procedure, unless he/she has been authorised to do so in writing by the organisation in respect of which he/she is carrying out the procedure and by SIQ;
- not to act in any way detrimental to the reputation or interest of SIQ or of the organisation with which it is cooperating in the certification procedure;
- to cooperate in any investigation procedure in the event of a suspected breach of these principles;
- to comply with the SIQ Code of Ethics.

3.3 Rules for applicants/customers

By signing the application/contract, the applicant/customer undertakes to:
- meet the requirements of the certification scheme, standards and regulations and any amendments to the certification scheme or standards or regulations under which the certification procedure was carried out;
- ensure that the certified services will continuously meet the requirements according to which the certification procedure was carried out;
- allow the certification staff to carry out certification and regular surveillance procedures without hindrance and to have access to the required documentation and records and the locations of the service, equipment, personnel, and subcontractors;
- allow the review of customer complaint records;
- allow the presence of observers, if necessary, during certification procedures;
- in the event of suspension or revocation of the certificate, immediately cease any reference to the certificate in promotional materials and take other actions required by the certification scheme (e.g., return of the original certificate);
- comply with the requirements for the use of conformity markings;
- in accordance with the signed application, collect complaints from customers and users of certified services, take appropriate actions and keep appropriate records of the actions taken, and forward the records of customer complaints and the records of actions taken to SIQ upon request;
- inform SIQ in a timely manner of any relevant changes affecting the certified service and its provision (e.g. legal/commercial/organisational status, change of ownership, changes in key management/decision-making/technical personnel, changes to the service and service provision, major changes to the quality management system);
- in EIDAS certification, in the case of major changes in technology or organisation, incidents or increased risks to services occur, communicate to the certification body the full circumstances of the events, in accordance with the instructions in this document and the signature on the AN303 application. The impact of the events shall be used to determine whether an additional audit is necessary. The reporting is the responsibility of the applicant/customer.

3.4 Confidential handling of data

SIQ undertakes to treat all information and data concerning the applicant for certification or the certificate holder as confidential and to use it exclusively in the performance of the procedures.

Information on the certification procedure and related activities shall be the business secret of the applicant or certificate holder and SIQ, with the exception of the granting or withdrawal of a certificate and a report to the Board of Certification Body in cases of any doubts concerning the certification, and the possibility of access to the documentation by the accreditation/notification bodies and supervisory authorities. Where SIQ is required by law to disclose confidential

information, or where it is contractually authorised to do so, SIQ shall inform the applicant/customer of the information provided, unless prohibited by law.

SIQ shall agree with the applicant or the certificate holder that SIQ shall have exclusive rights in respect of all documents delivered to the applicant/certificate holder.

4 General information on the certification procedure

4.1 Basic conditions for the issue of a certificate of conformity

- Only a company/institution that is officially registered in accordance with the applicable regulations may be the applicant for certification.
- The service or component for which the applicant wishes to obtain a certificate of conformity shall be clearly and unambiguously identified.
- An agreement shall be reached with the applicant on the standards, regulations or specifications that form the basis for the review and assessment of conformity.
- The certificate holder shall allow the certification body to carry out the certification process without interruption.
- The applicant shall confirm (e.g., by signing the application) that he/she is aware of and agrees to the provisions in CP207 or other documents describing certification procedures under different directives/regulations.

4.2 Activities in the certification procedure

a) Informative interview with the applicant
b) Identification of the applicant's requirements and/or preparation of the quotation
c) Service purchase order–as instructed and/or on SIQ forms or by a contract
d) Purchase order confirmation
e) Review and assessment of the adequacy of documentation
f) Audit planning
g) Audit implementation (Part 1, Part 2)
h) Audit report
i) Review of the audit report
j) Proposal for the issue of a certificate
k) Decision to issue a certificate
l) Communication with the applicant on the results and potential corrective actions
m) Settlement of financial obligations

Planning and conducting audits at the certificate holder.

4.3 Informative interview

The applicant's representative is briefed on the certification procedure and estimated costs. We also discuss the applicant’s requirements in detail. A quotation may be prepared.

In addition to the application forms (AN303) and the instructions for filling them in, the representative can also obtain other documents and publications with more detailed information on the procedures.

4.4 Application

The certification shall be ordered by the applicant either by the application form provided (AN303) or by acceptance of the quotation submitted.

The application/quotation relates to a specific service, a specific group of services, or a specific component, and identifies standards, policies or specifications, and regulations. It shall also contain clauses on the mutual obligations between the contracting authority and the contractor, in particular with regard to data confidentiality (the contractor – SIQ).

SIQ, after examining the documentation, requests that the application be supplemented if necessary. It may also issue a written confirmation that the application is complete.

The applicant is also informed of the cost of the certification procedure. The costs are estimated on the basis of the review of the application and the accompanying documentation and the envisaged procedure, and in accordance with the applicable price list. The application (purchase order) shall be confirmed in writing by SIQ.

By signing the application form (AN303), the certified service provider agrees to collect and act upon complaints from customers and users of the certified services and keep appropriate records of the actions taken, and provide the records of customer complaints and the records of the action taken to SIQ upon request.

4.5 Preparation and implementation of the audit

4.5.1 Audit planning

SIQ and the applicant shall agree on the date of the first audit. The audit shall be carried out at the applicant’s premises or partly remotely via videoconferencing. The length of the audit depends on the number of services or components that the applicant wishes to be certified. The applicant shall be informed by e-mail about the auditors, the audit, and the duration of the audit. In order not to interfere with the applicant's processes, we shall agree with the applicant who from the applicant's staff needs to be present at the audit and how the IT audit shall be carried out. Where the scope of the service assessment is a component, the audit team shall only assess the requirements defined for the individual services provided by the components.

Where the assessment requires the presence of observers (e.g., assessment of auditors, accreditation audits, etc.), SIQ shall inform the applicant/certificate holder of that in advance and the applicant shall allow their presence.

Once the certificate is issued, surveillance audits are carried out every 24 months.

The audit consists of two parts. The first part of the audit reviews the adequacy of the documentation, while the second part is aimed at sampling the procedures that shall comply with the applicant's documentation.

4.5.2 Pre-certification audits

4.5.2.1 Part 1 audit

The first part of the audit shall always be carried out at the applicant's premises or remotely via videoconference links, according to a pre-defined schedule. In addition to the auditor, at least one representative of the applicant shall be present.

The kick-off meeting introduces the participants, the audit process, and the objectives.

In the course of the audit, the auditor interviews relevant staff, and reviews procedures and practices, and documentation. If something cannot be reviewed or confirmed during the visit, the applicant shall be obliged to provide the auditor with supporting evidence within a maximum of five working days. The time taken by the auditor to prepare records shall also be included in the audit time.

At the final meeting, the auditor shall present the results of the audit, taking into account that sufficient time is allowed for discussion of the findings, corrective actions, recommendations, and questions from the applicant. At the meeting, the next steps shall be agreed upon and confirmed.

To avoid misunderstandings, all services are first interviewed and then the said is confirmed in practice during the second part of the assessment. The method of validation is for the auditor to observe a representative of the applicant operating the system, testing the operation of the system, inspecting the IT system settings, or showing evidence in some other way.

The audit is based on the scope of the services, using the following methodology:

The first part of the assessment shall last 8 hours, regardless of the number of services, the number of employees of the applicant working in the area of trust services, and the locations where these services are provided.

4.5.2.2 Part 2 audit

The audit shall be carried out at the headquarters of the applicant or partly via videoconferencing. The applicant shall be informed by e-mail about the auditors, the conduct, and the duration of the audit. In order not to interfere with the applicant's processes, we shall agree with the applicant who from the applicant's staff needs to be present at the audit, the tests to be performed and the services/processes to be audited.

The purpose of Part 2 audit is to check the applicant's arrangements by comparing the situation with the requirements set out in the regulations/schemes. The first audit is always carried out at the client's premises, according to a predetermined schedule. In addition to the auditor, at least one representative of the applicant shall be present at the audit.

The kick-off meeting introduces the participants, the assessment process, and the objectives.

In the course of the audit, the auditor shall interview relevant personnel, review procedures and practices, and carry out any tests that may be necessary. To avoid misunderstandings, all areas of the audit are first interviewed and then confirmed in practice. The recommended method of confirmation is for the auditor to observe a representative of the applicant operating the system/process or to show evidence by other means. The auditor may also test systems and processes.

At the final meeting, the auditor shall present the results of the audit, taking into account that sufficient time is allowed for discussion of the findings, corrective actions, recommendations, and questions from the applicant. At the meeting, the next steps are agreed upon and confirmed.

The second part of the assessment takes 6 hours for each service, with 3 hours for each additional service, 4 hours for each location where the central IT system for the provision of trust services is located, and 2 hours for sampling the reception points for the submission of applications for trust services.

Checklists are used for audit records and are annexed to the audit report.

4.5.2.3 Report

It shall contain the following information:

- the scope of the audit, including a summary and the standards, specifications, and regulations against which the audit is being conducted;
- the information security risk analysis report;
- the audit plan;
- the audit queries considered, the rationale for their selection, and the methodology used;
- the areas covered by the audit, including requirements for services or components;

- positive and negative findings;
- details of any non-compliances found, supported by objective evidence.

4.5.2.4 Review of the report

The report preparation and verification shall be carried out in two successive stages:

The auditor prepares the first draft audit report and sends it to the applicant in an editable format for comments and approval. The auditor shall send the report in a manner that complies with the requirements for the protection of confidential information within 14 days from the audit.

The applicant shall review the audit report and endorse it by notification to the auditor. If the applicant disagrees with anything in the report, the applicant shall provide the auditor with comments and evidence. The auditor shall record any disagreements in the report or correct any misunderstandings. The auditor shall provide the applicant with the final audit report in a pdf format within a specified time limit.

The subsequent certification procedure is carried out on the basis of the final audit report.

4.5.3 Elimination of non-compliance

The auditee is responsible for correcting non-compliance, including planning, provision of resources, implementation, and any costs. In the case of at least one non-conformity recorded in the report, the auditee shall prepare a corrective action plan and deliver it to the auditor within two months from the audit.

4.5.4 Additional and surveillance full-scope audits

Additional audit

If at least one non-conformity is identified during the site audit, an additional audit is required. The additional audit shall apply the same audit criteria as the certification/surveillance audit, but may also be carried out by a documentation review. Whether the additional audit will be carried out at the applicant's site or by a documentation review depends on the availability of evidence and the possibility to review the corrective actions and their implementation in order to update the status of the corrective actions in the corrective action table/implementation plan accordingly. If major environmental changes have been required, a full-scope audit shall be carried out.

An additional audit shall also be carried out if there are major technological, organisational, or regulatory changes that would have a significant impact on the trust services, or if the current procedures would no longer be able to provide the trust services.

Surveillance audit

A surveillance full-scope audit is carried out every two years. The scope of the audit is the validation of all controls and their supporting evidence.

4.6 Review of the audit report/Assessment of compliance

The audit report and the information and statements in the audit report and/or other technical documentation shall be reviewed by the certification staff and, if satisfactory, a proposal for the issue of a certificate shall be made to the certification body.

4.7 Issuing a certificate

The decision to issue a certificate/attestation of conformity shall be taken by the Certification Commission for Management Systems, which issues a certificate/attestation of conformity.

If inadequacies/non-conformities have been identified during the certification procedure, the Certification Commission shall inform the applicant and propose appropriate corrective actions.

If the applicant is already a certificate holder, a new certificate shall be issued before the expiry of the previous certificate, taking into account the time taken by the applicant to eliminate any non-compliance.

4.8 Monitoring changes to standards and regulations

Where there are changes in standards and/or requirements for certification procedures, or where services (or standards) no longer comply with the regulations, the Certification Commission for Management Systems shall set a time limit within which the certificate holder shall bring its service into compliance with the requirements of the new standard or regulations.

5 EU trust certification mark

Once the certificate has been awarded, the certificate holder may use the EU trust mark. In doing so, he/she shall comply with the rules in document CR303, which is published on the SIQ website.

The EU trust mark can be used in colour or black and white.

The reference colours for the EU trust mark for qualified trust services are:
- in four-colour printing:
  - Pantone Nos 654 and 116; or blue (100 % cyan + 78 % magenta + 25 % yellow + 9 % black)
  - and yellow (19 % purple + 95 % yellow),
- when using RGB colours, the reference colours are:
  - blue (43 red + 67 green + 117 blue) and
  - yellow (243 red + 202 green + 18 blue).

The EU trust mark for qualified trust services may be used in black and white only in cases where it is not practicable to use colour.

If the EU trust mark for qualified trust services is used on a dark background, it may be used in the negative using the same background colour.

If the EU trust mark for qualified trust services is used in colours on a coloured background which makes it difficult to see, a border around the EU trust mark for qualified trust services may be used to improve the contrast with the coloured background.

The EU trust mark for qualified trust services in colours:

The EU trust mark for qualified trust services in black and white:

6 Publications related to certificates

Care shall be taken to avoid confusion or even misleading publications (advertisements) relating to certificates of conformity. It is particularly important to make it clear which services are certified.

The certificate holder shall not use the certificate in a misleading manner or in a way that would bring SIQ into disrepute.

If the certificate holder wishes to publish only part of the audit report, he/she shall have the written consent of SIQ.

In information to its customers, the certificate holder shall not refer to features, rights, or the like in a way that could mislead customers, for example by making them believe that the characteristics of the service or its use are covered by the certificate when in fact this is not the case.

The interested party receives information on the certificate issued after submitting a request to the department. If the certificate holder does not wish the details of his/her certificate to be made publicly available, he/she shall inform SIQ in writing.

SIQ publishes information on the certificates issued on its website.

7 Withdrawal/revocation of a certificate

7.1 General

Revocation of a certificate can prevent a loss of trust in SIQ certificates and SIQ certificate holders. The Certification Commission for Management Systems monitors the use of certificates as part of its work. If it finds that there are grounds for revoking a certificate, it may revoke or withdraw the certificate.

The revoked certificate shall be removed from the list of valid certificates and the certificate holder and the supervisory authority shall be informed thereof.

A certificate may be revoked or withdrawn if, in the course of auditing/monitoring the use of certificates, it is found that there has been misuse or other breaches of the rules and regulations for certification.

In such cases, we inform the certificate holder that SIQ will revoke the certificate after a certain period of time, usually from 30 to 60 days. Within this period, the certificate holder may either correct the irregularities found and provide SIQ with evidence of this, or lodge an appeal/complaint.

The certificate holder shall have the right to appeal the decisions of the Certification Commission for Management Systems to the Appeals Commission of the Board of Certification as described in CR105, which is published on the SIQ website.

The Certification Commission may publicly announce the withdrawal of a certificate, stating the reasons for the withdrawal.

7.2 Grounds for revocation

The certificate of conformity may be revoked if it turns out that the service was not in fact in compliance with the prescribed technical requirements:

- for subsequently discovered facts that could jeopardise the validity of the certificate, which become apparent during the use of the service or through further investigations,
- for misuse of the certificate.

The certificate may also be revoked:

- if the services no longer meet the regulatory requirements, or if the standard/regulation on which the certification procedure was based changes and the certificate holder is unwilling or unable to ensure compliance with the new requirements of that standard/regulation,
- if the reference is used for services that have not been subject to a conformity assessment procedure;
- if the certificate holder does not wish to maintain the certificate,
- if the service is no longer provided,
- if incomplete or false information is provided in connection with the service;
- if significant changes to the service or to the management system have not been reported;
- if the certificate holder fails to comply with the requirements set out in the audit report;
- in case of bankruptcy or closure of the certificate holder's business,
- if the licensee fails to meet agreed financial commitments.

7.3 Procedure for the revocation of a certificate in order to replace it with a new one

Should the defect be such as to jeopardise the conformity of the service, the Certification Commission for Management Systems may revoke the certificate before issuing a replacement certificate, otherwise, the certificate shall be revoked when a new certificate is issued for the same service.

8 Misuse of a certificate

SIQ monitors the use of the certificates. If it finds that the certificate holder is misusing a certificate, it will take corrective action, including legal action if necessary. Misuse of a certificate may also result in revocation and cancellation of the certificate.

It is a misuse of a certificate of conformity if:

- at any time it appears that the applicant has misled SIQ in any way during the certification procedure;
- the certificate holder misleads buyers by claiming a certificate of compliance for a broader group of services on the basis of a certificate awarded for one or a few services, or by referring to a certificate for non-certified services;
- the certificate holder applies procedures to the service that have not been verified at the audit;
- the certificate holder makes any misrepresentation in relation to the certificate.

A certificate granted for a specific service shall be revoked by the Certification Commission for Management Systems if, in the course of its supervision, it finds that the certificate has been misused or that there has been any other breach of the provisions of this document and other documents specifying the certification procedures.

The Certification Commission for Management Systems may:

- propose appropriate corrective actions to the offender;

- revoke the certificate;
- publish the misuse in the mass media;
- take legal action if necessary.

The Certification Commission for Management Systems shall deliver a written reasoned decision to the certificate holder who has misused the certificate. The implementation of the decision taken shall be supervised by the Chairperson of the Certification Commission for Management Systems

The Certification Director shall ensure that all records relating to the resolution of the matter are properly filed.

The Commission may decide to revoke the certificate immediately or impose a time limit, not exceeding 3 months, on the certificate holder to revoke the certificate. Within this period, the certificate holder shall either eliminate the non-conformities identified and demonstrate this to the Certification Commission for Management Systems, or lodge an appeal/complaint, which shall be accepted or rejected by the Appeals Commission.

The certificate holder shall have the right to appeal the decisions of the Certification Commission for Management Systems to the Appeals Commission of the Board of Certification Body, as described in CR105, which is published on the SIQ website.

9 Handling complaints and appeals

The applicant/certificate holder may complain about inadequate work of SIQ or appeal the decision of the Certification Commission for Management Systems.

Any appeals against the work of the certification staff or the decisions of the Certification Commission for Management Systems shall be received by the SIQ Managing Director.

Complaints about the work of SIQ are dealt with in the first instance by the Certification Director. The complainant shall be informed in writing of the receipt of the complaint and the decision. This decision may be appealed to the Appeals Commission, which is a second-instance body whose decision is final.

Complaints about the management system of a certificate holder, which may be made in writing by anyone, shall be dealt with according to the same procedure as complaints about the work of SIQ. The complainant and the certificate holder shall be informed of the progress and conclusion of the complaint.

Appeals against decisions of the Certification Commission for Management Systems shall be made in writing by the applicant within 15 days of the receipt of the decision. The applicant shall document the appeal accordingly. The appeal shall be considered by the Appeals Commission, whose decision shall be final, in accordance with the document Appeals against the Decisions taken by Certification Commission, Notified Body and Inspection Body (CR105).

If the complaint/appeal takes a long time to resolve, we will inform the applicant of the progress of the complaint/appeal. If the complaint or appeal is justified, the Department Director(s) shall ensure that the grounds for the complaint/appeal are addressed.

The appeal procedure is described in more detail in document CR105 and published on the SIQ website. Other disputes are resolved by the court of subject matter jurisdiction in Ljubljana, Ljubljana Unit. The applicable law of the Republic of Slovenia shall apply to all relations.

10 Contact persons

Basis for certification	Contact person	Phone
EIDAS	Sabina Bauman	+386 1 4778 222
Certification of management systems	Miloš Seražin	+386 1 4778 212
Certification	Bojan Pečavar	+386 1 4778 210

E-mail addresses: name.surname@siq.si
When entering the first and last name, omit the semicolons.