University policy for the use of the remote digital signature

Version 1.0

The holder of a remote signature certificate is the person to whom the University of Trento has issued a remote digital signature certificate.

The registration authorities are members of the University who, upon delegation of the certification authority, identify the applicants for the purpose of issuing, revoking or suspending the certificates.

The certification authority is the organization that provides the qualified digital signature service pursuant to the Italian digital administration code.

The remote digital signature is a particular type of OTP based (One Time Password) digital signature. When signature certificates are issued, holders can choose to receive the OTP on their mobile phone by SMS, the Aruba APP or token.

Remote digital signatures are secure and guarantee the integrity and immutability of the electronic document on which they are placed. In this way, the signatures can be traced back to their authors.

The digital signature can be used to sign digital documents in the context of all the institutional activities that holders perform and in compliance with the signing powers granted by the law or by internal regulations of the University.

Holders undertake to:

Università degli Studi di Trento
P.IVA – C.F. 00 340 520 220
www.unitn.it
● store the personal codes necessary for remote signing in a safe place to avoid unauthorized use
● be the sole user of the signature
● use the signature only for teaching and research, and institutional administrative activities
● take appropriate organizational and technical measures to avoid harm to others
● provide the certification authority with accurate and truthful information regarding personal data as part of the initial registration process and promptly inform the registration authorities of any change in the contractual relationship with the University and of the data required for issuing the certificate.

The registration authorities:

● identify any new holders
● oversee the issuance of certificates
● revoke and/or suspend qualified certificates
● monitor certificate renewal activities
● send the list of certificates to be renewed to the certifying authority
● update the holders’ data when they change and transmit the new data to the certifying authority.

When a certificate is revoked it immediately ceases to be valid, regardless of its expiration date. This does not affect the validity of the certificate and of the signatures it provided before its revocation.

Certificates are revoked when:

● the holders cease to be employed by the University for any reason (eg. retirement, resignation);
● the holders no longer hold the position, qualification or institutional
role for which they were issued the certificate;
  ● the signature device is lost, stolen or replaced;
  ● security codes are lost or stolen;
  ● there is reason to suspect forgery or abuse;
  ● a violation of the rules has been committed by the user.

When a certificate is suspended, it is only temporarily unavailable.

Certificates are suspended when security codes are thought to have been lost.