Two-factor authentication

Two-factor authentication represents simple and effective way how to **increase level of security for** CAS **login**. Combination of a classic password and another, independent element of authentication, e.g. hardware key, significantly decreases risk of an unauthorized account access even in the event of your password getting compromised. This safety measure protects user accounts as well as sensitive data accessible via CAS.

Moreover, the two-factor authentication is simple and accessible. **Logging into your account remains quick** while ensuring the system grants access to authorized personnel only. Due to higher demands on cybersecurity is this form of authentication required by growing number of systems and its implementation into CAS is an important step towards protection of the university environment.

It is suggested to activate two different types of two-factor authentication in case one of them becomes inaccessible. **We recommend** use of **mobile app CU Key** combined with **text message code** as a backup. If you require further assistance with two-factor authentication settings, please get in touch with your local IT support.

Please select from the following options
(Combination of CU Key and Text message code is recommended)