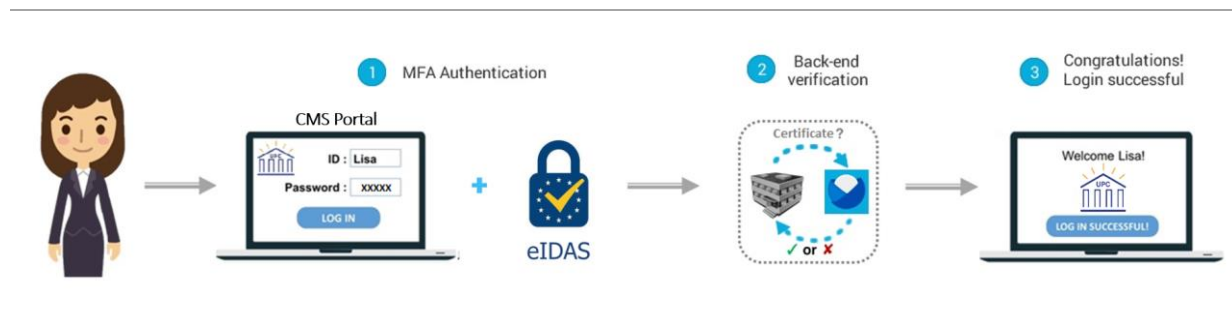


The UPC implementation team is pleased to announce a major milestone in the implementation of the Case Management System (CMS).

As of the end of October 2022, the CMS authentication process will be based on a strong authentication scheme. An electronic IDentification certificate (eIDAS) will be required as a second authentication factor to complement the current account + password system.



The new authentication eIDIAS scheme will provide the highest level of security while the use of private electronic ID (electronic signing certificate) will enable electronic signature of UPC documents.

The requirement for the electronic ID is set to qualified electronic certificates (pursuant to Art. 3(12) eIDAS regulation (EU) No 910/2014). Such level of certificate provide the strongest requestor identification process as well as ensuring a full legal recognition of the signature (using a qualified signature certificate and a qualified signature creation device). No other type of signature will be recognized and accepted.

Any person interested in creating an account in the CMS shall acquire a certificate based on the here-above requirement to an authorized provider. The list of these providers can be found on the EU Trust Services portal (<https://esignature.ec.europa.eu/efda/tl-browser/#/screen/home>).

Please consider that qualified electronic certificates do require a strong identification process. Such process usually imposes the physical presence of the requestor during the identification. However, some providers are certified to use "online" identification means (like video conferencing) but for a limited choice of qualified signature creation device. Providing such vendors are certified and recognized by competent national authorities.

The implementation of the strong authentication module will be activated by the end of October 2022.

Should you have any question on this communication, do not hesitate to contact us.

<https://www.unified-patent-court.org/contact>