



“Because we have multiple login systems and many different login scenarios to support, it is a relief that we can solve all our user authentication needs with the new platform and be compliant to the strict regulations set forth by the law makers.”

Martin Schimmel System Administrator, DTU

DTU is recognized internationally as a leading university in the areas of technology and the natural sciences and is known for its business-oriented approach, its focus on sustainability and its appealing study environment.

Leaving the hardware tokens behind

Today, DTU is ranked as one of the foremost technical universities in Europe. It continues to set new records in publishing, in the partnerships it develops with industry and in assignments undertaken by DTU's public sector consultancy. DTU's IT service function serves a wide range of departments, university entities and affiliated companies who benefit from their modern IT setup and infrastructure.

Employee remote access from across Europe is enabled through a number of login systems including Citrix, Cisco, and SSH. At first, the users accessing these systems were required to carry around hardware tokens for authentication when logging in. But the token-based setup was becoming increasingly time consuming to manage and was causing frustration for both users and the IT team managing the solution. Martin Schimmel, System Administrator at DTU explains: “The hardware tokens were a huge overhead for system administration. With more than 1000 token users, we constantly had tokens that needed to be replaced.”

Making life easier for IT

CensorNet Multi-Factor Authentication (MFA) was identified as the ideal solution to support DTU's security requirements and the advantages have been clear.



Customer

DTU (Technical University of Denmark)



Industry

Education



Challenge

To provide 1400 employees with secure access to a wide range of systems and applications, and to protect sensitive data processed by Computerome, Danish national super computer.



Systems protected

Citrix NetScaler, Cisco ASA VPN, SSH Gateway, Computerome (Super computer)



Solution

CensorNet Multi-Factor Authentication (MFA)

“Life is much easier now that the tokens are gone, and we have seen significant cost savings by migrating to CensorNet MFA. The tight integration to Microsoft Active Directory also makes it easy for us to manage and add users on the fly,” Martin explains.

Securing access to “Computerome”

Since the initial implementation, the use of CensorNet MFA has also been expanded to cover user authentication of around 400 scientists accessing DTU’s super computer named Computerome. Computerome is currently listed as number 236 of the top 500 most powerful super computers in the world and is used to process large amounts of data for scientific research in medicine and biology. Given the fact that Computerome stores and processes patient data, it was vital for DTU to add multi-factor authentication protection in order to meet regulatory requirements around storing health care data. The Computerome users are stored in an OpenLDAP directory.

Martin concludes: “Because we have multiple login systems and many different login scenarios to support, it is a relief that we can solve all our user authentication needs with the new platform and be compliant to the strict regulations set forth by the law makers”.

CensorNet Ltd.

Network House, Suite 6.01
Basing View, Basingstoke
RG21 4HG, UK
Phone: +44 (0) 845 230 9590
Email: sales@censornet.com

CensorNet A/S

Park Allé 350 D
2605 Brøndby, DK
Phone: +45 70 22 55 33
Email: sales@censornet.com

CensorNet Inc.

11801 Domain Blvd, 3rd Floor
Austin TX 78758, USA
Phone: +1 888 440 8456
Email: sales@censornet.com

