For English, scroll to page 5….

Inhoud

Aangescherpte inlogprocedure privacygevoelige systemen

Binnen de TU Delft moeten we de beveiliging van onze systemen op orde hebben. Het beschermen van uw en onze gegevens heeft dan ook een zeer hoge prioriteit. Om deze veiligheid te kunnen blijven waarborgen wordt de inlogmethode, die we nu hanteren voor de bedrijf kritische en privacygevoelige systemen, aangescherpt. Daarnaast vragen de nieuwe richtlijnen van de Autoriteit Persoonsgegevens (AP) op basis van de Wet Bescherming Persoonsgegevens om een sterke aanscherping van de beveiliging.[i]

Inloggen met 2FA. Hoe werkt dat?

BasWare

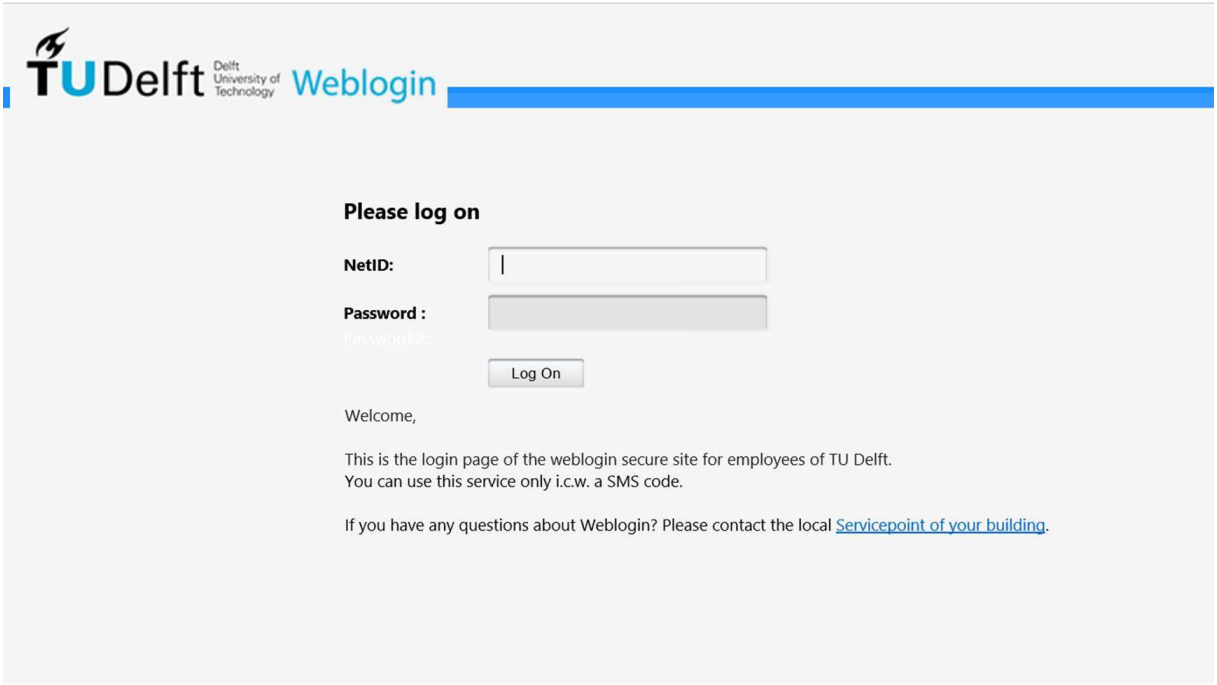
BasWare benadert u op de wijze waarop u dat altijd doet. Deze applicatie herkent zelf of u probeert in te loggen van binnen of buiten de TU Delft. Naargelang uw locatie zal u gevraagd worden regulier (gebruikersnaam + wachtwoord) of sterk (gebruikersnaam + wachtwoord + SMS authenticatie) in te loggen.

ERP-LN, Peoplesoft en Osiris voor backoffice-medewerkers

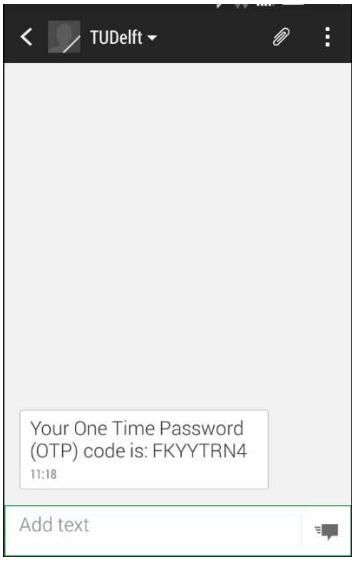
Indien u binnen de TU Delft de applicaties ERP-LN, Peoplesoft of Osiris voor backoffice-medewerkers wilt opstarten, dan kunt u dat blijven doen zoals u dat gewend bent. Voor toegang van buiten de TU Delft zal de reguliere weg worden afgesloten. Indien u van buiten de TU Delft de applicaties ERP-LN, Peoplesoft of Osiris voor backoffice-medewerkers wilt opstarten, dan moet u dat doen via de link https://webloginapps.tudelft.nl

Inloggen met 2FA

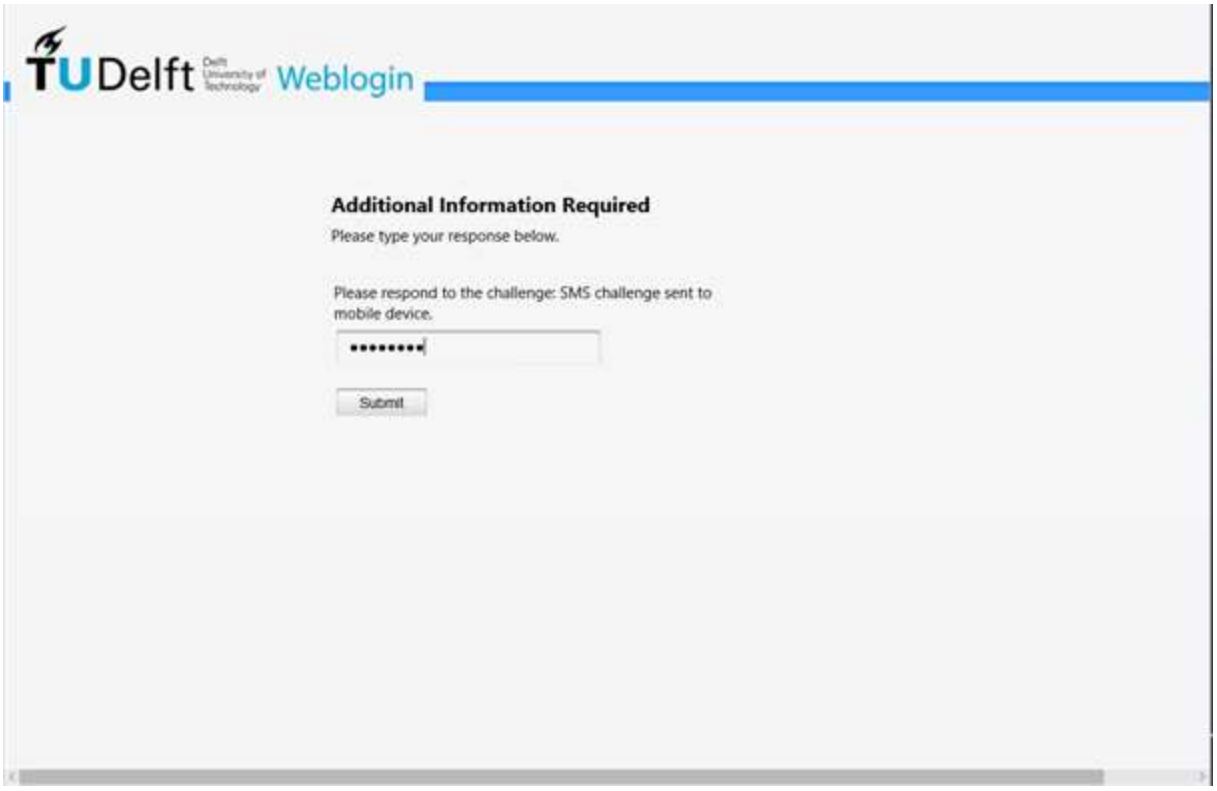
Wanneer u van buiten de TU Delft op een 2FA beveiligde https://webloginapps.tudelft.nl applicatie gaat inloggen, dan ziet u het volgende scherm:



Hier logt u in met uw NetID en wachtwoord. U ontvangt op uw telefoon een SMS bericht met daarin de extra toegangscode:



Deze toegangscode vult u vervolgens in op het onderstaande scherm:



U drukt op “Submit” en u wordt ingelogd.

Wat betekent het voor u?

1. Als u van buiten de TU Delft inlogt op een bedrijf kritische of privacygevoelige applicatie zal er straks om een extra controle van uw identiteit gevraagd worden.

2. **Voor 2FA moet uw mobiele nummer bij de TU geregistreerd zijn**. Dit kun u doen via het digitale loket E-Service op https://e-service.tudelft.nl. Let op: u kunt deze registratie alleen doen als u binnen de TU Delft inlogt op https://e-service.tudelft.nl. Het SSC ICT wil benadrukken dat het mobiele nummer standaard alleen wordt gebruikt voor SMS-authenticatie en contact bij verzuim[ii]. Er zijn in Nederland geen kosten verbonden aan het ontvangen van SMS berichten.

3. **Om 2FA te kunnen gebruiken, moet de Functioneel Beheerder van de applicatie u toevoegen aan een speciale gebruikersgroep.** Neem hiervoor contact met deze functionaris op.

Wanneer wordt 2FA ingevoerd?

Op **1 januari 2016** wordt 2FA ingevoerd voor **BaswareIP, BaswarePM, ERP-LN, Peoplesoft en Osiris voor backoffice-medewerkers**. Naar aanleiding van de verscherpte wet- en regelgeving rondom medische gegevens hebben gebruikers van het HR systeem **VerzuimXpert**, de applicatie voor ziek- en herstelmeldingen, sinds 30 augustus jl. te maken met deze manier van inloggen. Voor VerzuimXpert geldt dat er geen onderscheid wordt gemaakt tussen toegang van binnen of buiten de TU Delft.

Andere bedrijf kritische systemen zoals Digiforms, TIM, etc. volgen in een later stadium. Op deze applicaties logt u zowel binnen als buiten de TU Delft in zoals u nu gewend bent.

Meer informatie

Het ‘dubbel’ inloggen zal in het begin voor iedereen wennen zijn en mogelijk ongemak kunnen veroorzaken. Dat begrijpen we heel goed, maar een betere beveiliging van onze systemen is in ieders belang, ook in dat van u. Als u vragen heeft over deze nieuwe manier van inloggen, dan kunt u contact opnemen met het Servicepunt in uw faculteit.

Improved log-in procedure for privacy-sensitive systems

At the TU Delft, we must ensure that our systems are properly secured. As such, an extremely high priority is given to protecting both your and our information. In order to allow us to maintain our high security standards, the current log-in procedure for business-critical and privacy-sensitive systems is being improved. The new Personal Data Authority (AP) guidelines, based on the Personal Data Protection Act, also call for major improvements to security.[iii]

Logging in with 2FA. How does this work?

BasWare

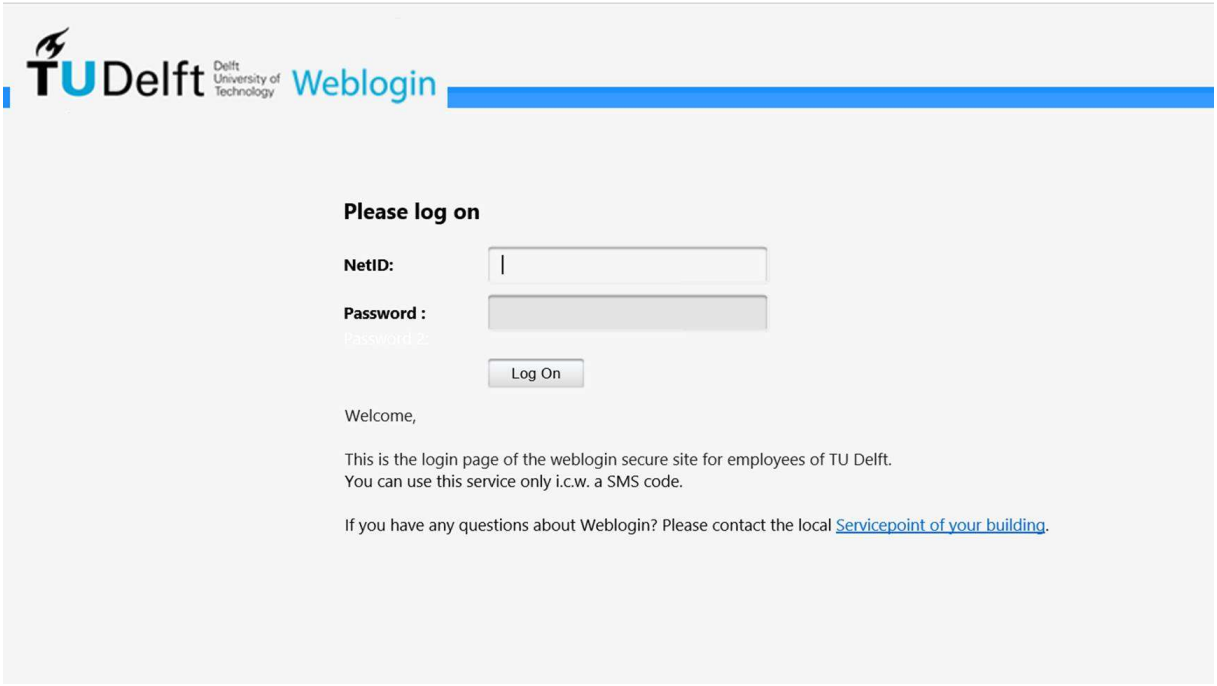
BasWare can be accessed in the same way as in the past. This application detects if a user is logging in from within the TU or from outside. Depending on your location, you will be asked to log in normally (user name + password) or by using the more secure method (user name + password + SMS authentication).

ERP-LN, Peoplesoft and Osiris for backoffice employees

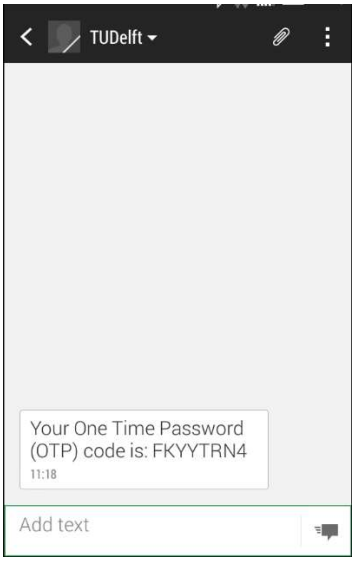
If you want start the applications ERP-LN, Peoplesoft or Osiris for back office employees within the TU Delft, you can continue to do so in the manner you are accustomed to. The regular method will no longer be applicable for access from outside the TU Delft. When starting the applications ERP-LN, Peoplesoft or Osiris for back office employees outside TU Delft, use the link https://webloginapps.tudelft.nl

Logging in with 2FA

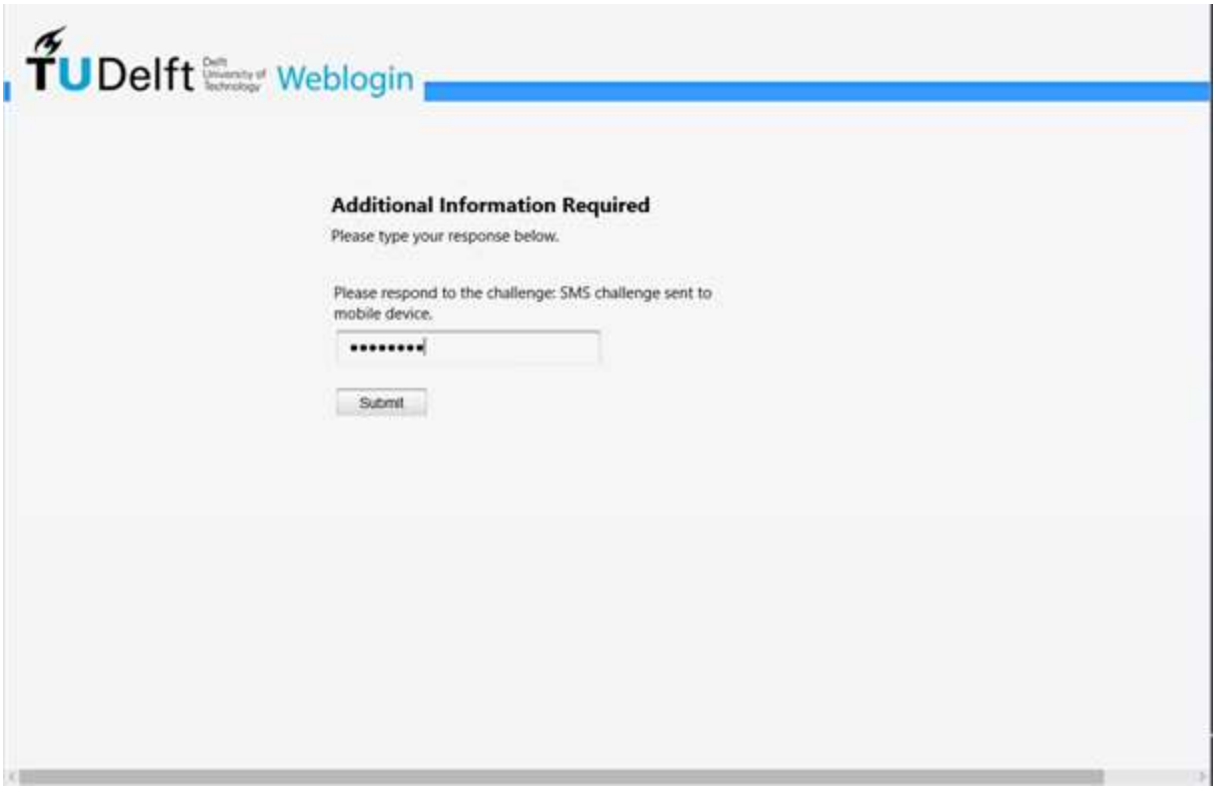
When you log in to a 2FA-secured https://webloginapps.tudelft.nl application outside the TU Delft, you will see the following screen:



Log in here using your NetID and password. You will receive a text message to your phone containing the extra access code:



This access code must then be entered on the screen below:



Click on "Submit" and you will be logged in.

What does this mean for you?

1. If you log in to a business-critical or privacy-sensitive application outside of the TU Delft, you will be asked to complete an additional verification of your identity.

2. **In order to use 2FA, your mobile phone number must be registered with the TU Delft.** You can register your number via the E-Service digital service desk at https://e-service.tudelft.nl.Please note: you can only register if you log in within TU Delft on https://e-service.tudelft.nl. SSC ICT would like to emphasise that the mobile telephone number stored in the system is used for authentication and contact in case of absenteeism[iv]. No costs are associated with receiving text messages (SMS) in the Netherlands.

3. **Before you can use 2FA, the Functional Administrator of the application must add you to a special user group.** Please contact the Functional Administrator to arrange this.

When will 2FA be implemented?

2FA will be implemented for **BaswareIP, BaswarePM, ERP-LN, Peoplesoft and Osiris for back office staff** on **January 1, 2016**. As a result of the tightened legislation and regulations related to medical data, the users of the HR system **VerzuimXpert**, the application for illness reporting and reporting back to work, have had to log in this way since 30 August 2015. No distinction is made between access within and access from outside the TU Delft when using VerzuimXpert.

Implementation for other business-critical systems such as Digiforms, TIM, etc. will follow at a later date. You can log in to these applications in the manner you are accustomed to, both within and outside the TU Delft.

Additional information

Everyone will undoubtedly need time to adjust to the 'double' log-in process, and it may initially cause some inconvenience. We are well aware of this, but improving the security of our systems is in everyone's interest, including your own. If you have any questions about this new way of logging in, please contact the Service Desk at your faculty.

---

[i] Twee-Factor Authenticatie, of **2FA**, is een veilige manier van inloggen op systemen die informatie bevatten die beter beschermd moet worden dan alleen met een gebruikersnaam en wachtwoord. Er wordt voor de toegang tot een applicatie (= authenticatie) een zogenaamde *tweede factor* gevraagd, die de gebruiker "*heeft*" in plaats van "*weet*". De gebruikersnaam en het wachtwoord zijn zaken die een gebruiker "weet". De tweede factor is een eenmalig en tijdgebonden "token" dat aan de gebruiker wordt verstrekt op een device dat de gebruiker fysiek in bezit heeft, i.c. een SMS bericht op de mobiele telefoon, op het moment dat de gebruiker inlogt.

[ii] De gebruiker kan dit mobiele nummer in e-service wel publiceren, waardoor het in het TU telefoonboek zichtbaar wordt.

[iii] Two-Factor Authentication, or **2FA**, is a safe method of logging in to systems containing information that needs a higher level of protection than just a user name and password. A so-called *second factor*, which the user *"possesses"* instead of *"knows"*, is required to gain access to an application (=authentication). The user name and password are things that the user *"knows"*. The second factor is a one-time and time-synchronised "token" that is supplied to the user on a device that the user physically possesses when he/she logs in. In this case, the token is a text message sent to the user's mobile phone.

[iv] The employee can however publish this mobile number in e-service, which makes it visible in the TU telephone directory.