



# BETROET PLATFORM (TRUSTED PLATFORM)

De fleste nyere computere har et TPM modul (Trusted Platform), dvs. en chip, som gør det muligt at lagre biometrisk information (ansigtsgenkendelse eller fingeraftryk) eller en kode, der giver nem og sikker adgang til diverse beskyttede funktioner, såsom JSIS online.

Se nedenfor, hvordan man etablerer og bruger en Trusted Platform på en computer, iPad eller tablet.

## 1 – INDSTILLINGER - WINDOWS


Klik på Windows symbolet  nederst på din skærm, åbn **Windows Indstillinger**  og vælg **Konti**.


Under **Indstillinger for logon**, vælger du blandt de tre Windows Hello muligheder den, der svarer til den måde, du normalt bruger til at få adgang til dit apparat: Windows Hello Face eller Fingerprint eller Windows Hello PIN. Vælger du PIN, skal du nu konfigurere din Windows Hello kode, som skal være den samme som den, du bruger til at få adgang til dit apparat (vælg evt. "Skift" og indsæt samme kode igen). Du kan blive bedt om din Microsoft adgangskode.

Den betroede platform vil kun virke på det Windows apparat, hvorpå den er aktiveret. Hvis man har en Google-konto og slår synkronisering til, vil man dog kunne benytte sin TPM på alle enheder, hvor man er logget ind med Google.

## 1 – APPLE (den præcise terminologi kan variere afhængigt af model)

Accepterer du synkronisering mellem dine Apple apparater, skal du kun etablere den betroede platform på ét af dem, for at den virker på alle dine Apple apparater – **vælg det nyeste**.

**iPad**: Åbn **Systemindstillinger**  og vælg **Adgangskoder**. Er Adgangskoder låst, indsætter du blot din kode og klikker dig videre. Tjek under **"Indstillinger til adgangskoder"** (til højre), at du har aktiveret **"Autoudfyld adgangskoder og loginnøgler"** og **Adgangskoder/iCloud nøglering** (og en evt. foretrukken browser).

**MAC**: Åbn **Systemindstillinger**  - **Generelt**. Klik (til højre) på **"Autoudfyldning og Adgangskoder"** og tjek, at **"Autoudfyld adgangskoder og loginnøgler"** og **"Adgangskoder"** (eller **Nøglering/Passwords**) er slået til. Tjek også, at muligheden er aktiveret for at **låse din Mac op** og **autoudfylde adgangskoder** ved biometri eller med en kode.

## 2 – AKTIVERING TIL EU LOGIN (WINDOWS OG APPLE)

Åbn **MyRemote** via <https://myremote.ec.europa.eu/>, log ind og klik på **EU Login**.

Vælg **Manage my Security Keys and Trusted Platforms** → **Add a Trusted Platform**. Giv apparatet et navn, så du kan genkende det (Min Lenovo / iPad ...) og klik på **Submit**.

Autentificér dig på normal vis (biometrisk med ansigtsgenkendelse/fingeraftryk eller med din adgangskode).

Administrerer du flere EU Login konti, skal hver enkelt konto aktiveres som beskrevet.

### 3 – BRUG MED EU LOGIN

Log på f.eks. <https://mypmo.europa.eu/>. Indsæt email og password på anmodning og vælg **"Security key or Trusted Platform"** som verifikationsmetode. Autentificér biometrisk eller med din adgangskode, og du er inde!

### 4 – EU LOGIN PASSWORD

Ved etableringen af den betroede platform giver du/Windows/Apple tilladelse til at administrere dine adgangskoder. Når dit EU Login password skal fornyes (hver 6. måned), skal du sikre dig, at det samtidig bliver opdateret i mappen med adgangskoder under **Indstillinger** i dit apparat.