



Båstad kommun

IDM & IGA

Mats Pålsson
IT-driftansvarig
Kommunikation och digitalisering



Båstads kommun – En växande kustkommun med framtidstro

- Båstads kommun ligger på vackra **Bjärehalvön** i nordvästra Skåne och är känd för sin natursköna miljö, sitt aktiva näringsliv och sin attraktionskraft som boendeort.
-  **Antal invånare:** 16 026 personer per den 31 december 2024
-  **Antal anställda i kommunen:** ca 1 937
-  **Antal elever i kommunens skolor:** ca 2 200
-  **IT-avdelningen:** består av **1 chef** och **8 medarbetare** som ansvarar för drift, support och digital utveckling
- Kommunen har under de senaste åren haft ett tydligt flyttöverskott, vilket visar att allt fler väljer att bosätta sig i området. Med satsningar på bostadsbyggande, hållbarhet och digitalisering är Båstad en kommun i rörelse – både för invånare och verksamheter.



Uppdraget: Ny Mail





2022- då läge

- En åldrande IDM miljö
- Många specialskrivna integrationer i IDM
- ”Novell-baserad” Win10 miljö
- 50% av maskinparken äldre än 4 år
- Gammal nätverksinfrastruktur.
- Återkommande problem med lösenordsbyten
- Problem med uppkoppling till Wi-Fi, gammal 802.1x miljö
- Gafe plattform
- Jamf plattform



2026 Nu-läge

Ny IDM miljö

- Servrar i Båstad
- Support och underhåll från ID-North
- Två målsystem: AD+M365 och Passagesystem

Behörighetsportal - IGA

- Tilldelning via företagsroller
- Beställningsbara resurser
 - Filmappar
 - Applikationer
 - Passage till passageområden/dörrar
 - VPN grupper
- Ingen manuell beställning av behörigheter hos Internsupport



2026 Nu-läge

M365 miljö

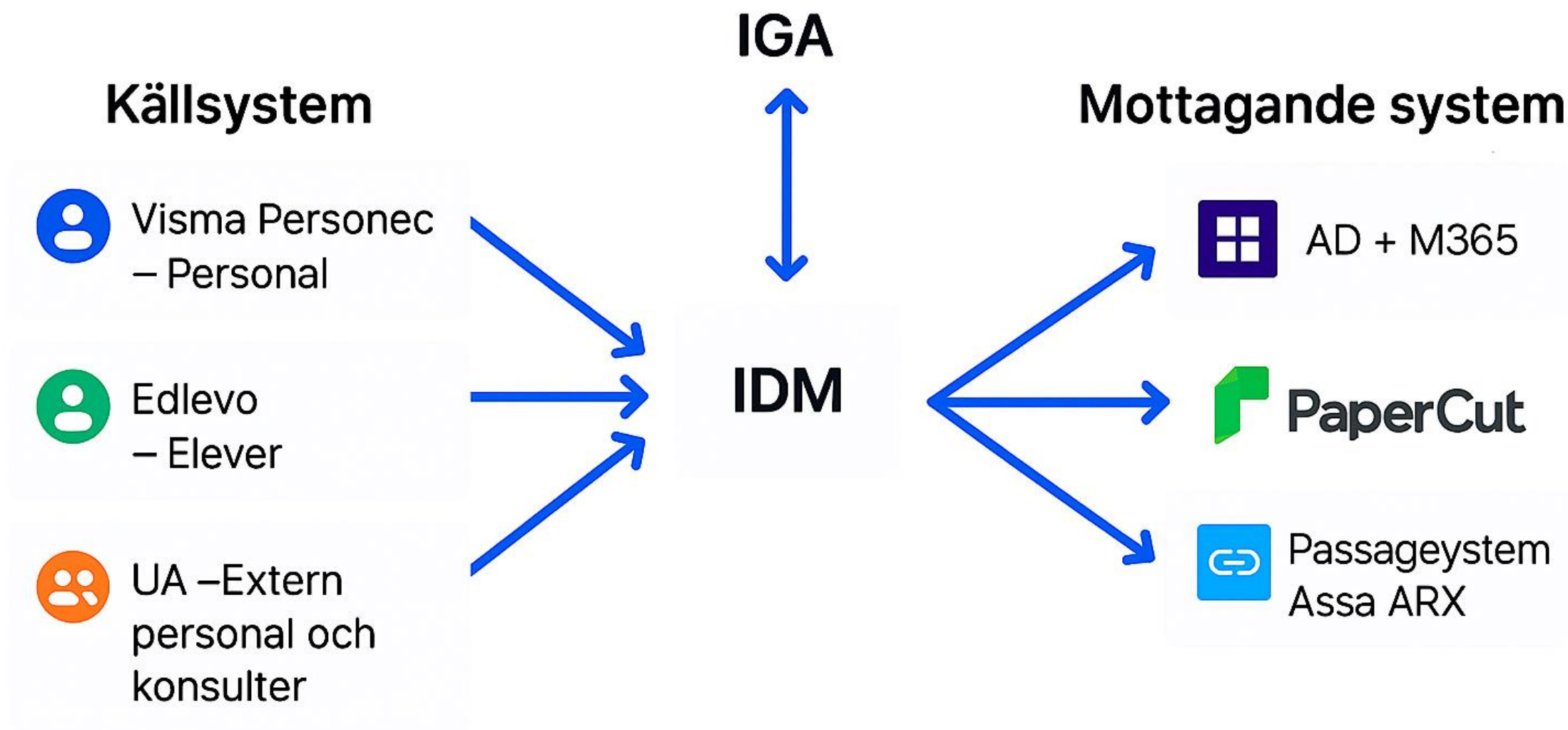
- Teams, Outlook
- Word, Excel, Powerpoint

Datorer

- Ca 850 PC med Win 11 med WHfB
- Ca 1000 Mac, 450 Iphone, 1800 IPad
- Lösenordsbyte med QR kod och BankID
- Ingen maskin äldre än 4 år.

Ny nätverksinfrastruktur

- Ny certifikatbaserad WIFI lösning.
- Segmenterat nät med en brandvägg per Site
- Nya Switchar med portsäkerhet
- Nya Accesspunkter och Switchar (90% klart)





IDM

Identiteter

Olika identiteter

- Anställda/Förtroendevalda, hämtas från HR system
- Elever, hämtas från elevregister
- Externa konsulter, beställningsformulär
- Externt anställda/Fastighetsbolag, beställningsformulär

Konton

- Ett konto per typ av Identitet
- Alla konton har ett slutdatum
- Manuella konton har max 1 års livstid, raderas automatiskt om det inte förlängs

Kvalitetssäkring

- Alla identiteter kvalitetsäkras mot skatteverket
- Manuell hantering av skyddade personuppgifter

Livscykelhantering

- IDM som hanterar alla identiteter.



IDM

Attribut enligt SKR

Attribut person

- Namn (grunddata från källsystem, Navet) ✓
- Personnummer (grunddata från källsystem, Navet) ✓
- Skyddade personuppgifter (grunddata från källsystem, Navet). ✓

Attribut anställd

- Användarnamn: Unikt användarnamn för inloggning. ✓
- Uppdrag eller tjänsteinformation(roll): Den kan innehålla chef, Befattning, skola, tjänst osv. ✓
- Organisation: Avdelning, befattning och tillhörande enhet. ✓
- AID-koder: En unik identifierare enligt SKR:s standard. ✓
- E-postadress: Primär e-postadress för kommunikation. ✓
- Chef: Vem som är ansvarig över e-identiteten. ✓
- Federationsattribut som behövs för till Skolfederation. ✓

Attribut politiker

- Användarnamn: Unikt användarnamn för inloggning. ✓
- E-postadress: Primär e-postadress för kommunikation. ✓

Attribut elev

- Användarnamn: Unikt användarnamn för inloggning. ✓
- E-postadress: Primär e-postadress för kommunikation. ✓
- Skolenhetskod: Relevant information om vilken skola eller utbildningsinstitution individen tillhör. ✓
- Federationsattribut som behövs för till skolfederation. ✓

Attribut övrigt (konsulter, hantverkare, entreprenörer)

- Användarnamn: Unikt användarnamn för inloggning. ✓
- E-postadress: Primär e-postadress för kommunikation. (tilldelas endast vid behov) ✓
- Uppdragsansvarig: Vem som är ansvarig över e-identiteten. ✓



Säker inloggning

Tier modell i AD

- 3 olika säkerhetsnivåer

Nätverkssäkerhet

- Varje site har en egen brandvägg
- Separerade nätverkssegment per funktion
- Portsäkerhet med identifiering och 802.1x för kabelansluten enhet
- Certifikatbaserat WIFI (Endast WPA2 Enterprise/WPA3)

Inloggningssäkerhet

- Windows Hello
- Ansikte/Finger/Pinkod
- Lösenord används bara vid uppstart av personlig dator och på delade datorer.
- MFA

SSO inloggning IDP

- +60 federerade tjänster
- Bankid/Siths inloggning till system med skyddsvärd information
- Egil/Scim SS12000 för hantering av lärare/elever i externa skolsystem
- Autoprovisionering av konton via SSO där Scim saknas
- JIT Provisionering (Just In Time) för medborgare.



IGA

Behörighetsportalen
Företagsroller

Företagsroller tilldelas via:

- AID koder
- Arbetsställenummer
- Källsystem (Personal eller Elevregister)
- Övriga attribut på identiteten

Företagsroller:

- Applikationsgrupper
- VPN-grupper
- Passageområde (en eller flera dörrar)



Behörighetsportalen Beställningsbart

Beställningsbara resurser:

- Delad mapp på Filserver
- Applikation på datorn
- Passageområde (en eller flera dörrar)

Beställare:

- Anställd
- Kollega
- Administratörer
- Chef

Godkännare:

- Närmsta chef
- Systemförvaltare
- Passageområdesansvarig
- 2+ stegs godkännande:
 - Närmsta chef
 - Systemförvaltare

Beställningar

- Påminnelse till godkännare var 5 dag
- Efter 21 dagar avslås beställningen.
- Start och slutdatum går att sätta men ej krav



Passagesystem

Flödeshantering

- 1 kort/tagg per anställd eller elev
- Kort registreras via Papecut kopiator
- Kortnummer skickas till passagesystemet inom 2 minuter
- Vid glömt kort/tagg kan lånetagg registreras via kopiatorn
- Endast ett kort eller tagg knuten till en identitet
- Passageområden tilldelas via IGA

Passage

- 320 passageområden
- 175 st beställningsbara
- 75 företagsroller som tilldelar passageområden



Revision

- Beställningsbara resurser revideras 2 gånger per år
- Revisionsperioden pågår under två månader
- Ansvarig chef, systemförvaltare eller passageområdesansvarig beslutar om behörigheten ska vara kvar eller ej.
- Ej bedömda behörigheter behandlas som nekad förlängning
- Vid avslutad revision raderas ej bedömda behörigheter.



Frågor?

Tack för ni har lyssnat.