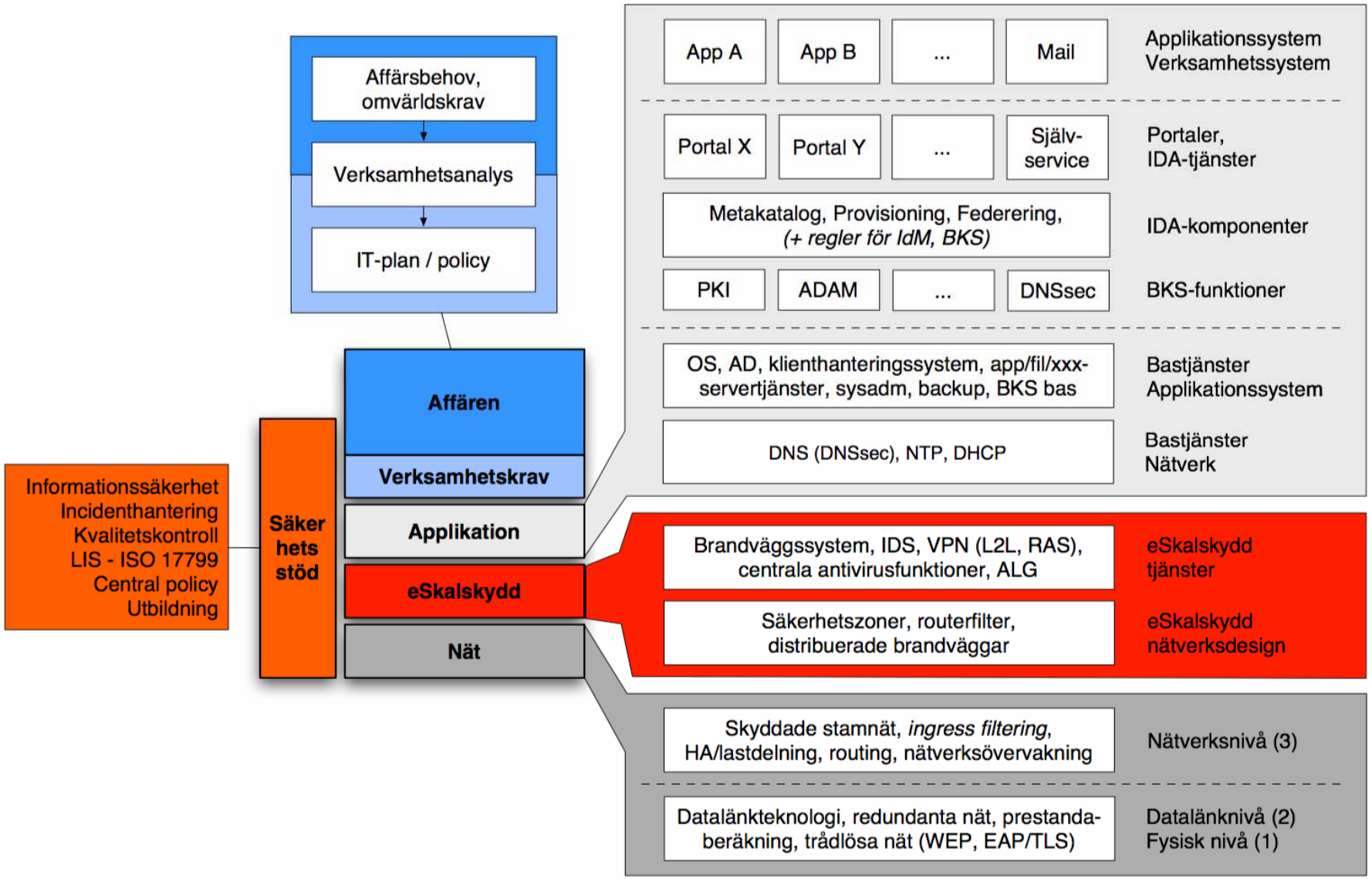
Identity Management
i ett nätverkssäkerhetsperspektiv

Martin Fredriksson

Varför IdM?

- Flera olika plattformar/tekniska system
  - Windows, AD, Unix, routrar, VPN, etc, etc
- Många olika informationssystem
  - Olika applikationssystem med olika säkerhetskrav, installerade vid olika tidpunkter
- Användarhantering
  - Olika användardata i olika system: PA, organisation, projekt, OS, databaser
- Målet:
  - Öka *säkerheten*
  - Sänka kostnaden för användarhantering

Modell för nätverkssäkerhet



Att förstå: behörighetskontrollsystem

- Autentisering
  - Säkerställa en identitet
  - Tre typer:
    - Något man **kan** (t.ex. lösenord)
    - Något man **har** (t.ex. smart kort)
    - Något man **är** (t.ex. fingeravtryck)
- Auktorisation
  - Tilldela rättigheter baserat på identitet
  - Ex: åtkomst till filer, rätt att ta ut pengar från ett konto, passagekontroll
  - RBAC: en användares auktoriserade roll(er) styr åtkomst
- Accounting (spårbarhet)
  - Loggning på olika nivåer

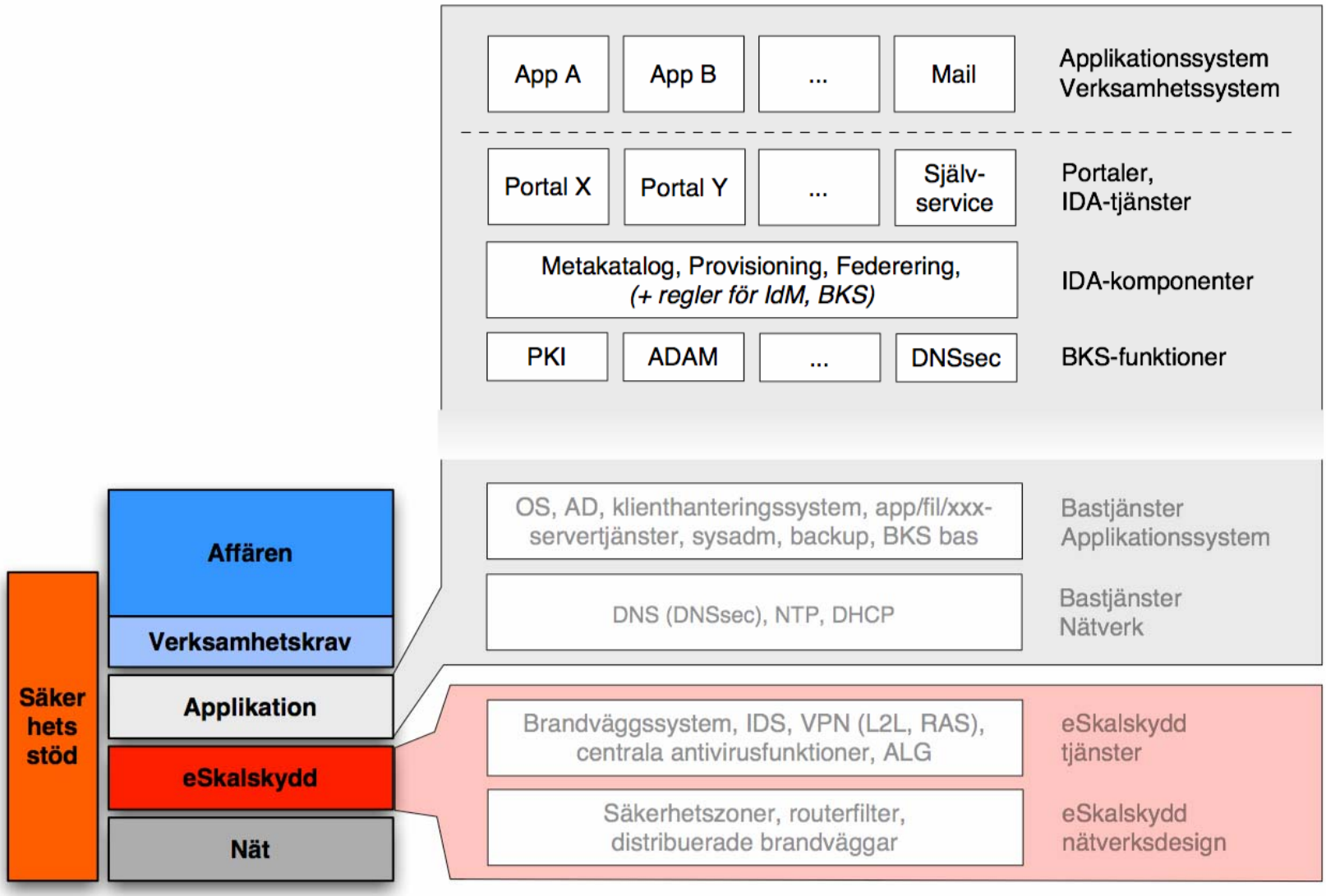
Att förstå: applicerad kryptografi

- Kryptoalgoritmer
  - Vilka är bra till vad? Hur starka behöver nycklar vara?
  - Konfidentialitet: kryptering (DES, AES, RC4, ...)
  - Integritet: kontrollsumma, signaturer (MD5, SHA-1, RSA)
- PKI
  - Certifikat, publika nyckel-system, smarta kort
- Nätverksprotokoll med krypto
  - SSL/TLS (HTTPS), SSH, IPsec, Kerberos, ...
- Vad krypteras?
  - Nätverk, session, meddelanden, dataposter ?

Att förstå: exekveringsomgivning

- Operativsystem
  - Vilken säkerhet erbjuds av operativsystemet?
  - Vilka säkerhetsfunktioner finns?
  - Åtkomst mellan processer?
- Prestanda
  - Hur mycket resurser får vi förbruka?
  - Vilka andra system exekverar på samma maskin?
- Övervakning, felhantering
  - Aktiva system för övervakning av applikationssystem

Modell för applikationssäkerhet



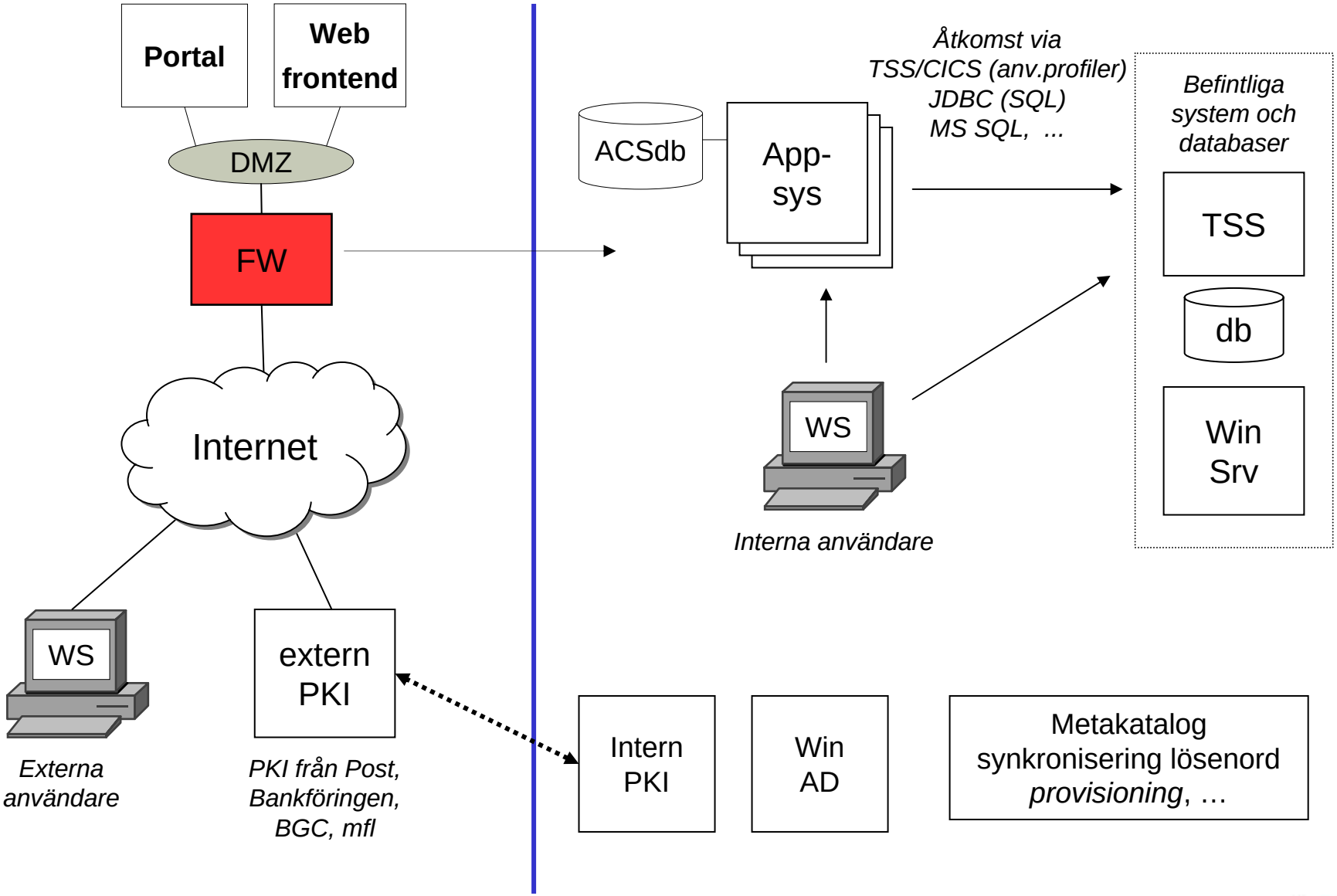
IdM: komponenter

- Single Sign On (SSO)
  - Egentligen: Reduced Sign On (ibland behövs högre krav…)
  - ETT lösenord att komma ihåg (högre kvalitet!?)
  - Eller ännu bättre: stark autentisering
  - 50-60% av helpdesk-kostnad är lösenordsrelaterad
- Lösenordssynkronisering
  - Byte av lösenord i ett verktyg (AD, självservice, etc) --> automatiskt byte av lösenord i andra system
- Provisioning
  - Hantering av användarkonton i flera informationssystem
  - Automatisering: skapa, ändra, stänga av konton, upptäcka icke använda konton, etc, etc
  - Kan vara svårt! Kräver kunskap om enskilda informationssystem och/eller ett gemensamt BKS-stöd-system (ofta beskrivs regler för detta i metakatalog)

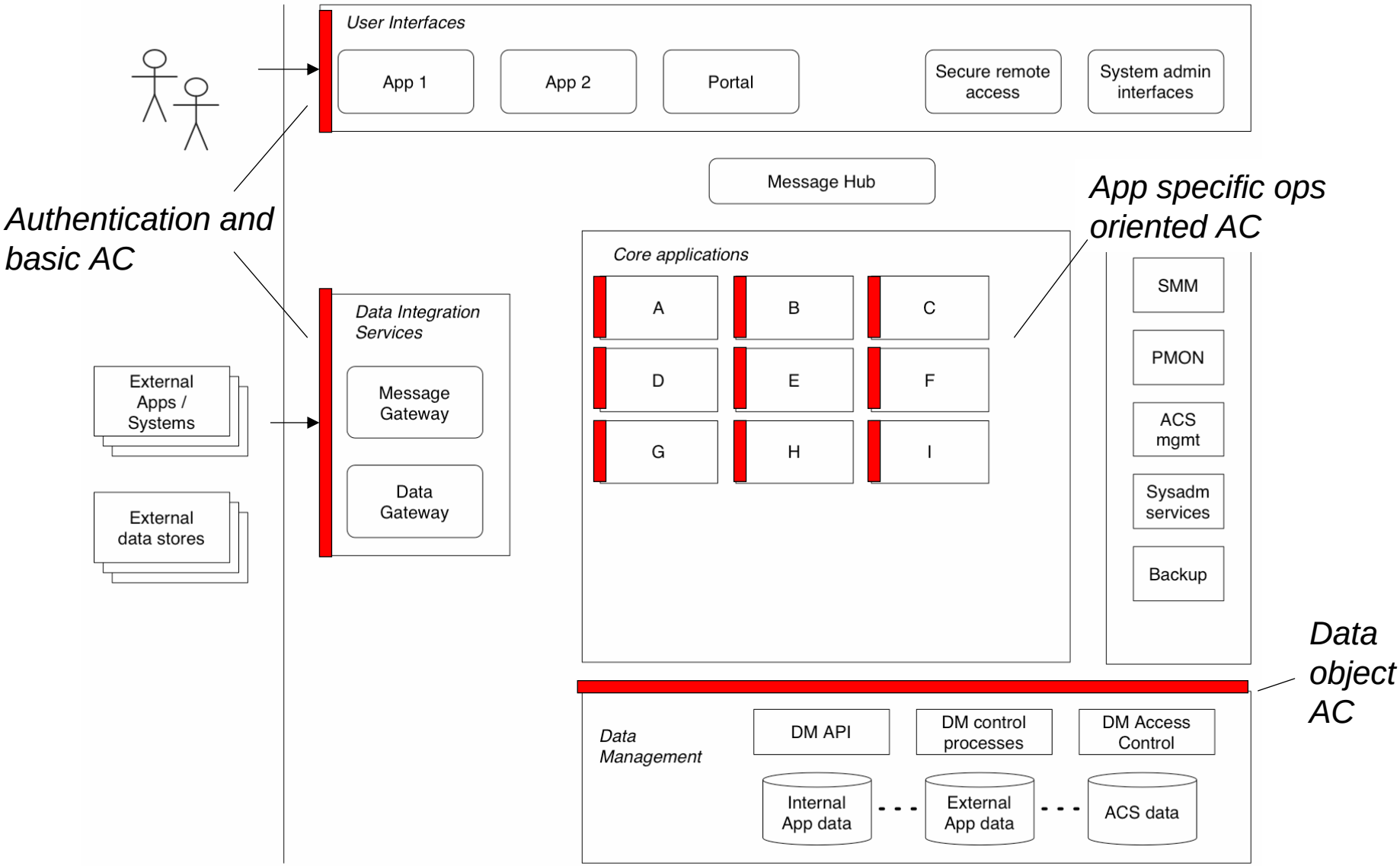
IdM: komponenter

- Självservice
  - Användare skall kunna administrera sitt eget konto, givetvis under styrning/kontroll av säkerhetspolicy
  - Triggar lösenordssynkronisering / provisioning
- Åtkomsthantering (*access management*)
  - Central styrning (och uppföljning) av regler för åtkomstkontroll i olika informationssystem
  - Svårt att genomför generellt! Kräver ofta centralt system.
  - Lämpligt att börja lite enklare, t.ex. med Windows AD och tillåta applikationsspecifika regler som utgår från samma uppsättning roller
- Federering (*federated identity*)
  - Godkännande av annan organisations identiteter
  - Kräver regler, avtal, etc
  - Baserat på PKI?

Exempel 1: PAS : modell för BKS, nätvy



Example 2: A & AC



Exempel 2: Authentication methods

- Public-key based
  - Smart card, or “soft card”
  - Both users and applications
  - Preferred method for web access from controlled terminals, for access from external applications, and for general admin access via SSH
- Token cards
  - One time password generators (SecurID, …)
  - Preferred method for access from external (e.g. public) terminals
- Username / password
  - When the other methods are not an option…
- Single Sign-On
  - Support for *pre-authenticated* users, via Kerberos

Exempel 2: Identity Management

- Highly dependent on existing access control infrastructure and on customer needs
- Requires risk / security analysis
- Synchronization with external ACS systems
  - Via meta directory
  - Directly with external ACS system
- Hooks for using external ACS systems
  - LDAP, Radius
- Self-service support
  - Support for existing self-service type applications

THE END