FEDERERING & AUTENTISERING I MOBILEN

Ur en arkitekts perspektiv och demo

MAGNUS LARSSON

2014.05.22 | CALLISTAENTERPRISE.SE

CALLISTA
– ENTERPRISE –

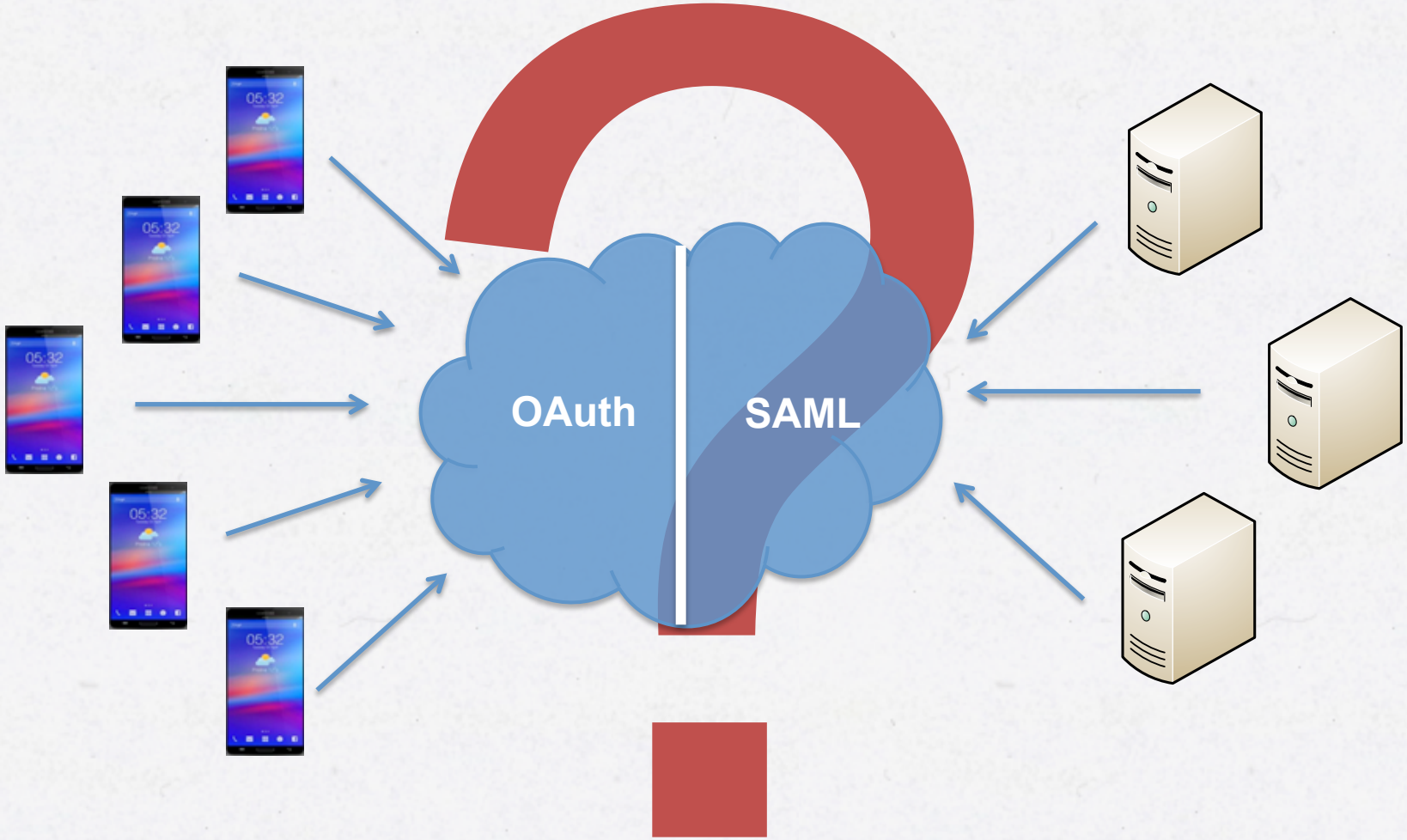
VILKA ÄR CALLISTA ENTERPRISE?

- Oberoende konsultbolag
  - Grundat 1997
  - Kontor i Göteborg och Stockholm
  - 30 konsulter och växande – Di Gasell 2014

- Fokuserar på
  - Tillämpad enterprise och applikations-arkitektur
  - Integration och frontend
  - Öppen källkod

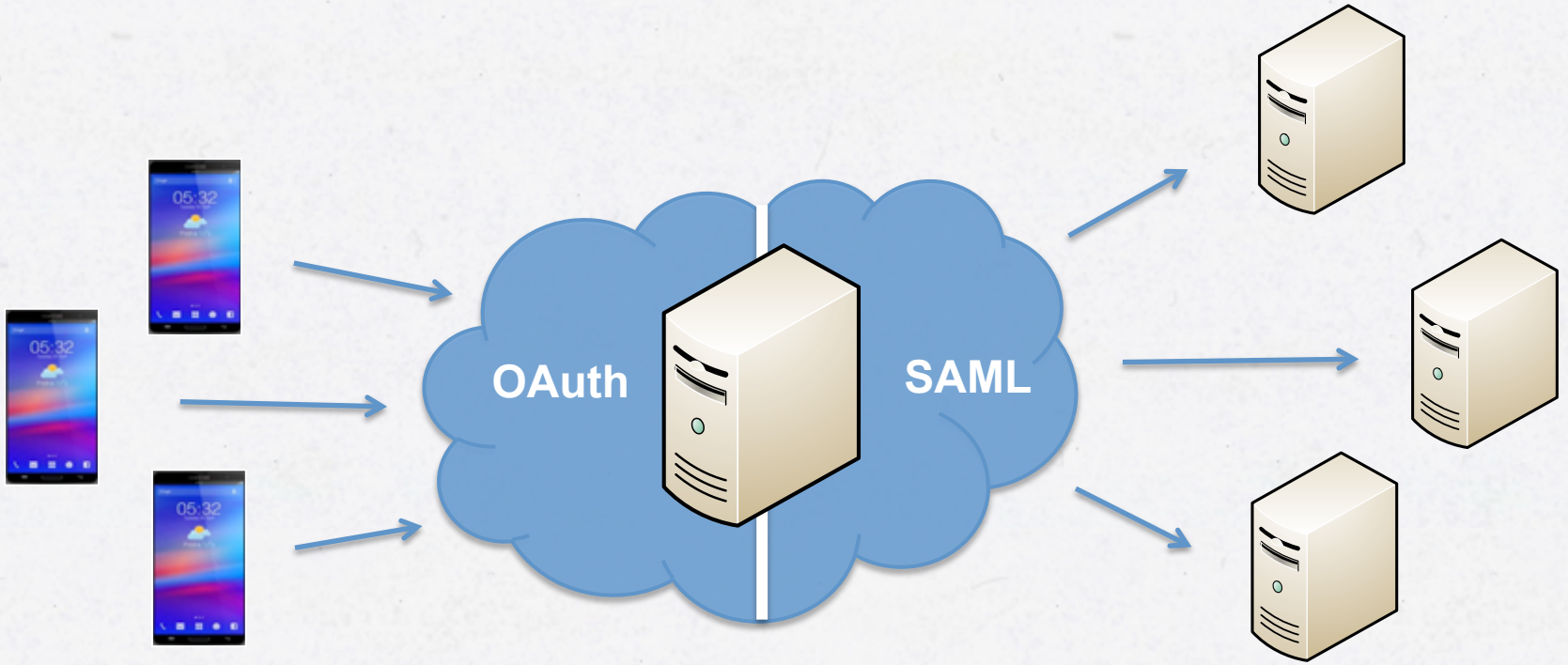
- Vår väg in i den federativa tillits-världen
  - Uppdrag inom vård och omsorg (sedan 2008)
    - » T-bok, RIV-TA, nationella tjänsteplattformen, SAMBI PoT
    - » Kunder: Inera, VGR och SLL

UTMANINGEN



CALLISTA
– ENTERPRISE –

LÖSNINGSFÖRSLAG



Mobile Apps

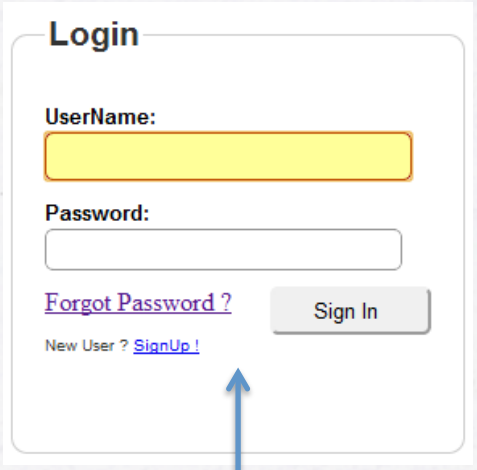
Security Gateway

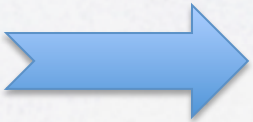
IdP's, SP's

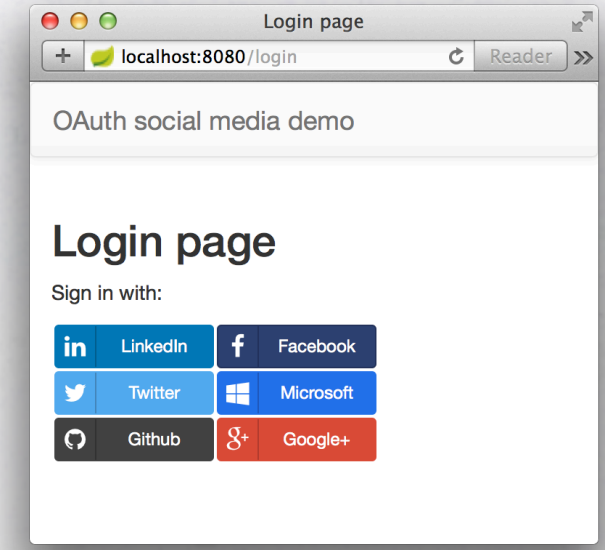
CALLISTA
– ENTERPRISE –

VAD ÄR OAUTH 2.0?

- En öppen standard för ett auktorisationsprotokoll
  - Användarstyrd behörighetskontroll
- Exempel på användning av OAuth: Social Login (utan federation)







User Credentials

  - Läs mer på blogg: http://callistaenterprise.se/blogg/teknik/2014/09/02/adding-social-login-to-a-website-using-spring-social/

MER OM OAUTH 2.0

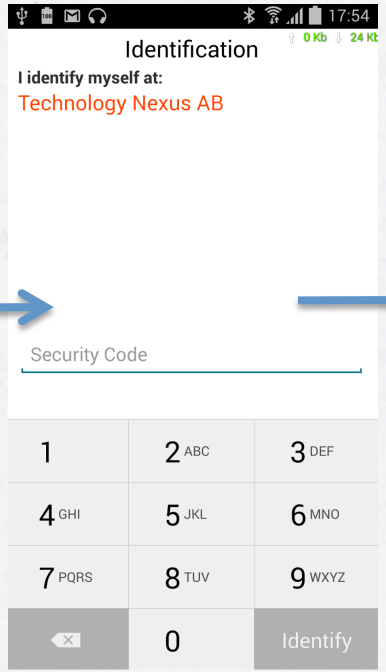
- Välbeprövat
  - Google, Facebook, Twitter, LinkedIn, SalesForce (100+ till finns på https://oauth.io/providers)
- I grunden enkla HTTP/JSON anrop
- Lättviktigt, passar mobila plattformar väldigt väl
- Plattformsoberoende
  - Ramverk finns för Java, MS .Net, Javascript, PHP, Python mm (se http://oauth.net/2/ och http://oauth.net/code/)
- Framtidssäkert
  - OpenID Connect bygger vidare på OAuth 2.0

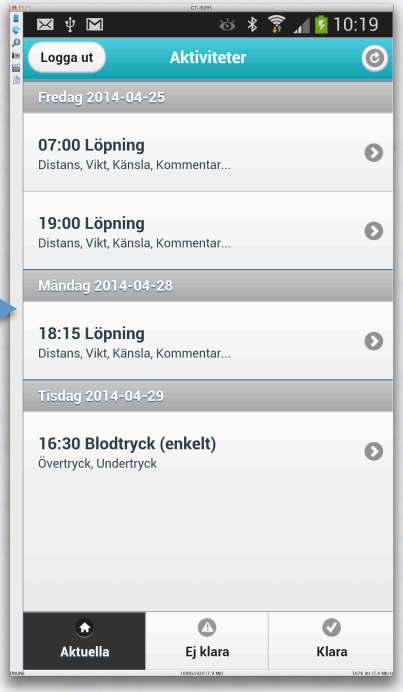
DEMO-DAGS!

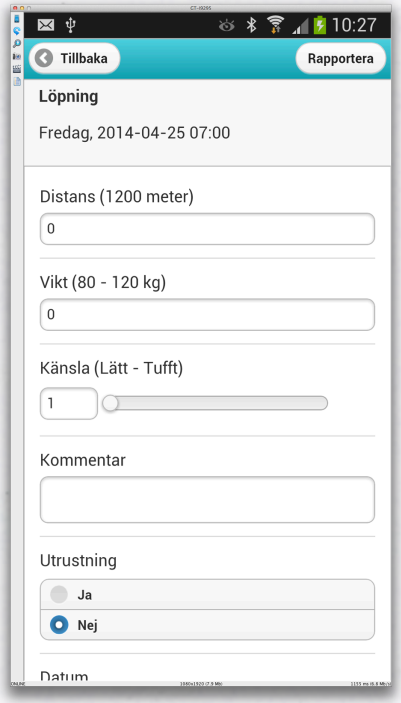
- Demonstration
  1. Byt autentiseringsmetod via konfiguration
  2. Single Sign On
  3. Single Logout

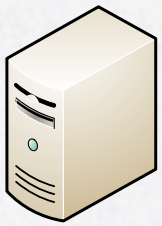
- Demo setup
  - Utgå från en befintlig mobil app
    - » Hårt integrerad med Mobilt BankID
  - Bryt loss val av autentiseringsmetod från mobil-app
    - » Delegera till en Security Gateway
  - **Mobil App:** Min Hälsoplan (Landstinget i Jönköpings Län)
  - **Security Gateway:** neXus Hybrid Access Gateway

BEFINTLIG MOBIL APP - MIN HÄLSOPLAN

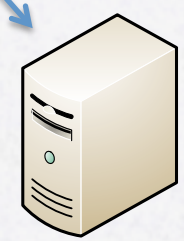








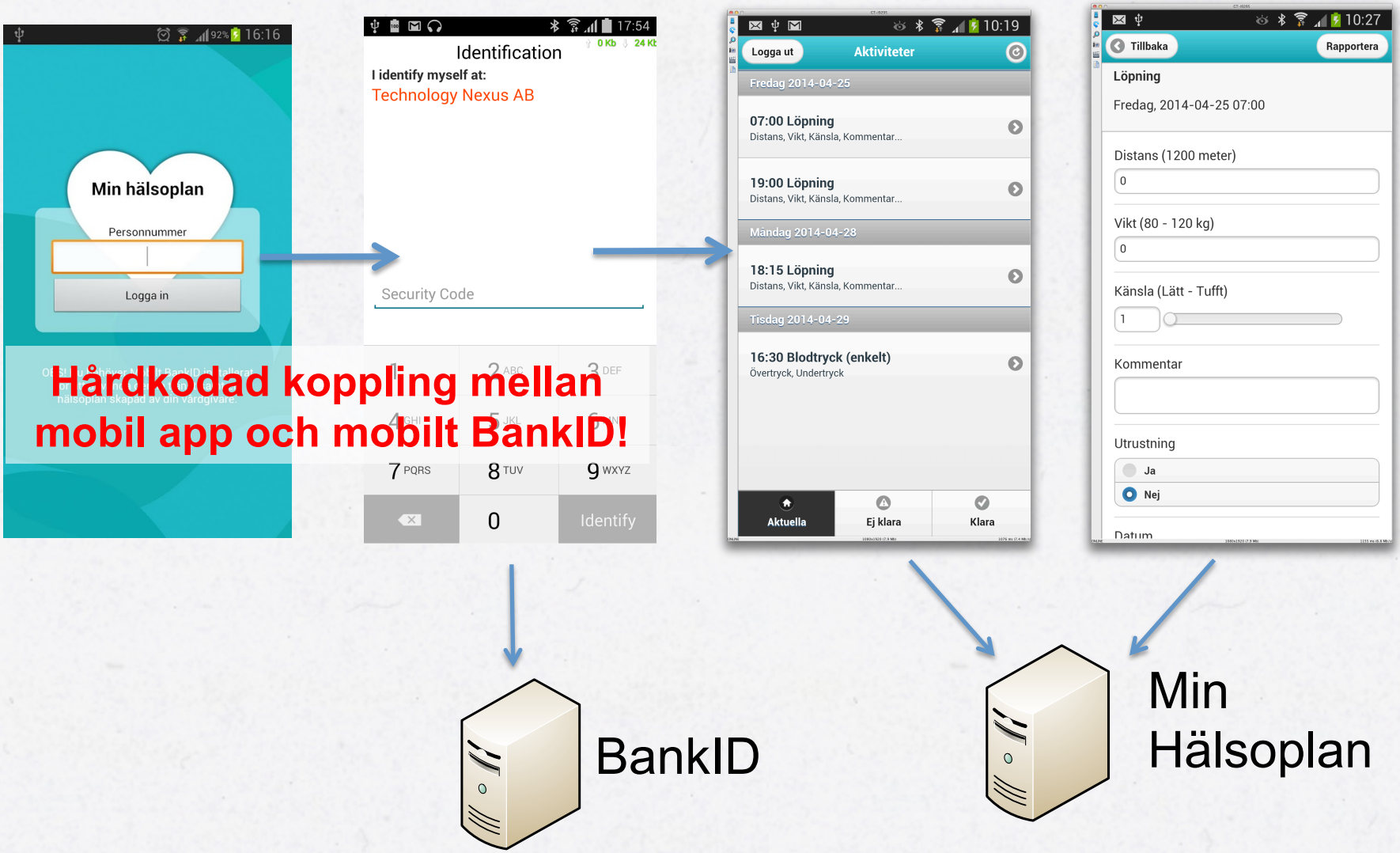
BankID



Min Hälsoplan

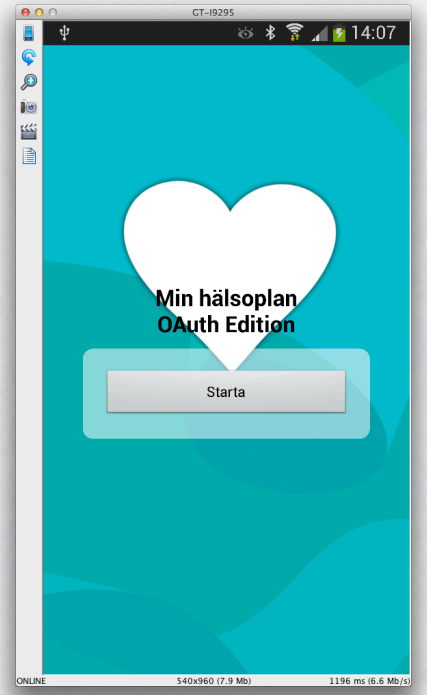
CALLISTA
– ENTERPRISE –

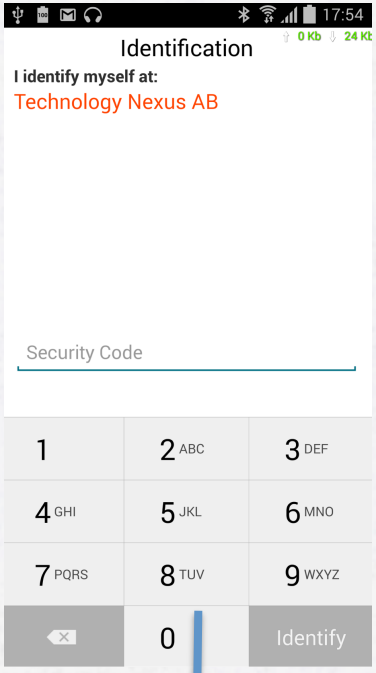
BEFINTLIG MOBIL APP - MIN HÄLSOPLAN

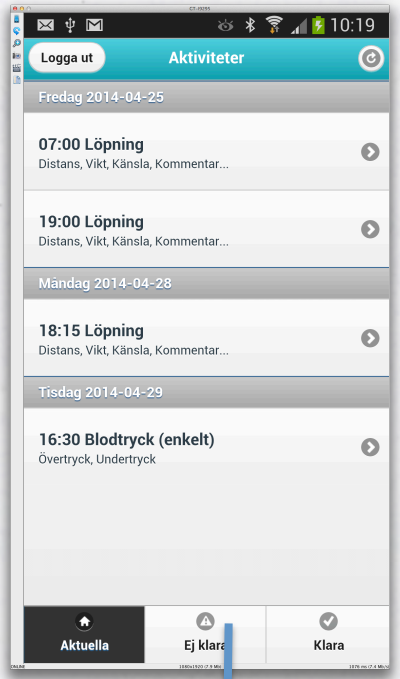


CALLISTA
– ENTERPRISE –

MIN HÄLSOPLAN - OAUTH EDITION

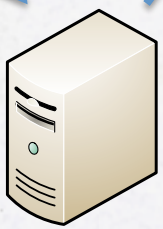




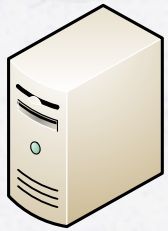


Security Gateway

BankID



Security Gateway



Min Hälsoplan

CALLISTA
— ENTERPRISE —

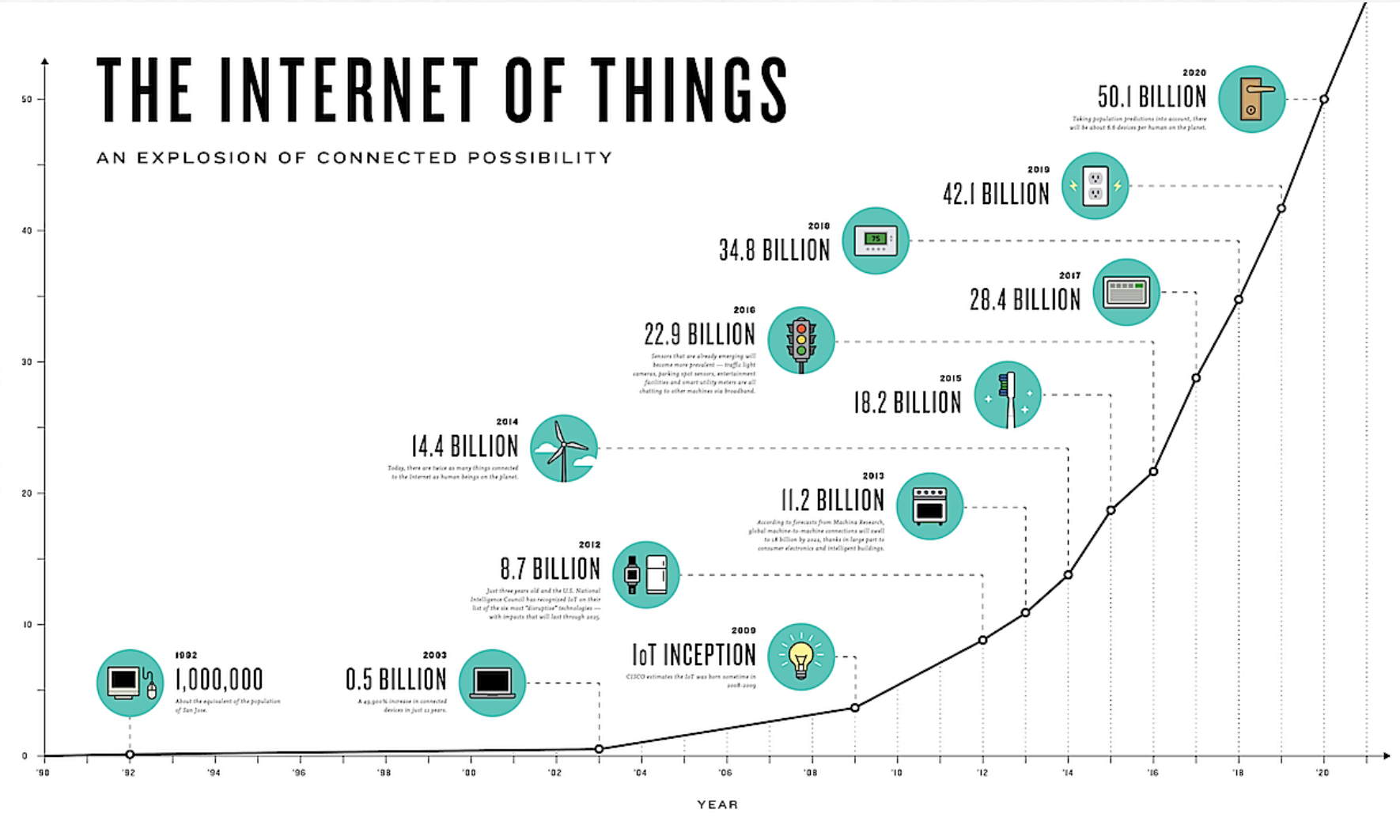
SUMMERING - FEDERERING & AUTENTISERING I MOBILEN

- Med SAML och ett sunt användande av OAuth 2.0 *kan man*:
  - Bygga vidare på befintliga SAML federationer
  - Mobila appar kan delegera identitetshantering och autentisering till federationens infrastruktur
  - Möjliggöra single sign-on och single logout
  - Möjliggöra användarstyrd behörighetskontroll
  - Prata med mobila enheter på mobila enheters vis
    - » Lättviktig OAuth/JSON istf tungviktig SAML/XML

SUMMERING - FEDERERING & AUTENTISERING I MOBILEN

- Ett sunt användande av OAuth 2.0 *kan möjliggöra* öppenhet:
  - Plattforms och produkt oberoende
    - » Map såväl språk som plattformar för servrar och mobila enheter
  - Interoperabilitet
    - » Enkel HTTPS och JSON
  - Väl beprövad teknik
    - » Speciellt inom sociala medier (Google, Facebook, LinkedIn…)
  - Inkluderande
    - » Vi kan stötta olika typer av mobila tillämpningar

UPPKOPPLADE ENHETER BLIR BARA FLER OCH FLER…



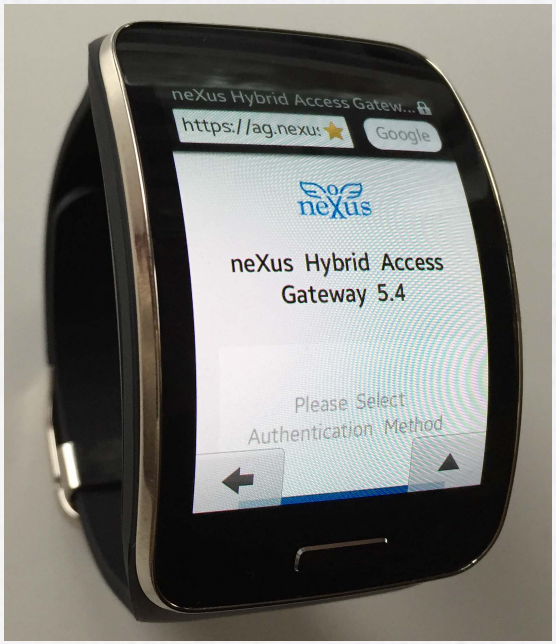
Source:

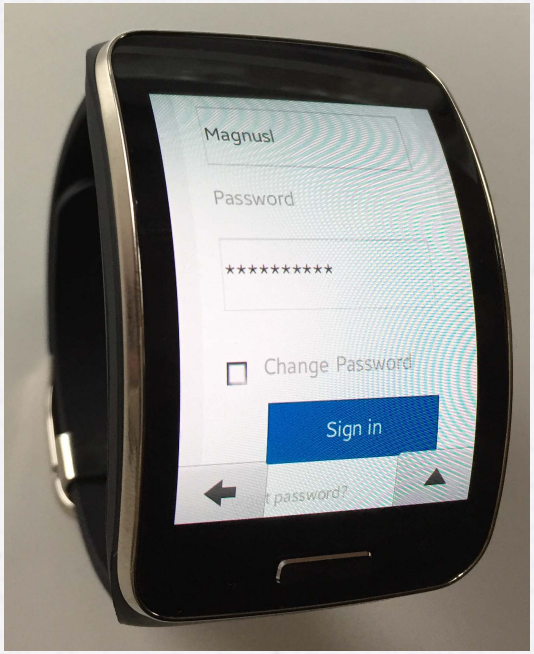
http://www.theconnectivist.com/2014/05/infographic-the-growth-of-the-internet-of-things/

… OCH MINDRE OCH MINDRE…

Exempel på ”smart klocka” med egen 3G, Wi-Fi, GPS, Web-läsare, Appar osv…

- Självgående, behöver inte närvaro av en mobiltelefon





CALLISTA
– ENTERPRISE –

Q&A