



Tillit i tid och otid

KommlTS, Karlstad, 2026-05-06

thomas@certezza.net



Värderingsstyrda

- Vi är ett oberoende informations- & cybersäkerhetsföretag som har erbjudit expertis till offentlig & privat sektor i 30 år.
- Vår vision är ett säkert & robust samhälle

En kompetent och oberoende informations- och cybersäkerhetspartner

- Säkerhetsskydd
- Juridik (AI, NIS2, GDPR, eIDAS mfl)
- Digital tillit (e-leg, e-underskrift)
- Styrning, risk och efterlevnad (GRC)
- Personalsäkerhet & säker rekrytering
- Identitet och behörighet (IAM)
- Kryptografi & PKI, PQC
- It-säkerhet
- Säkerhetscenter (Incident, MISP)
- Säkerhetstester (Red Team)

År 1996

- Sverige väljs in i FN:s säkerhetsråd för 3:e gången
- Internet slår igenom på bred front i Sverige
- Olympiska spelen firar 100 år i Atlanta
- Göran Kropp bestiger Mount Everest
- Certezza och KommITS grundades
- Carl XVI Gustav fyller 50 år
- Femtilappen återinförs
- Posten lanserar Torget



torget

presenteras av



fjärrkontroll karta

Tor 14 maj 1008

vinn
mobiltelefon
gratis cd-rom

dagens fråga:

Har du dator hemma?
Rösta!

Ja Nej ?
75% 10% 12%

sök på Torget:

Sökord:

sök

☞ tips

sök på företag:

Sökord:

Snyggare magasin

T-nytt: 10:33 Vagener åtalade för minkutsläpp



Hans Dahlman är Lelle Printer

här är printernet

- med de senaste telegrammen

gratis

- CD-rom till
medlemmar

shop it

- över 175.000

datorprodukter

gosa

- med ministern
vinn 10.000!

efterlys

- försvunna

kompisar

I cgmagotchi - vinn 10 000 kronor

sök på Lycos

PRAT: Eric Gadd 12/5 | Elitloppet, Sveriges största travtävling, 20/5 |

handla i dag



Rugby-
troja,
139:-

Josefsson

hästa
nätvaruhuset

Besök oss här!

Enligt
Internet-
guiden 4/1998



Stolnygg-
säck
149:-

Sportjoran

Nu 81 butiker online!

EVENEMANG: Eric Gadd live 12/5 | Lelle Printer | Wilmer X | Val 98

Nyheter:

II-NYTT:

Aktion mot
Microsoft?

Deltorgen i helgan:

ARBETE:

17.804 lediga jobb
just nu

BOSTAD:

Prata bostad
med andra

DATER:

Äventyr och action
i ett spel

FACHANDELN:

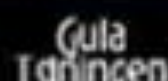
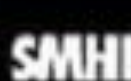
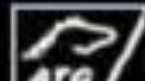
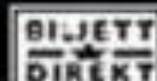
Fixa hemmet
med Järnia

FAMILJ&FRITID:

Kuratorn ger
goda råd

FINANS:

Så skaffar du
en aktiedepå



Tillit i tid och otid

Låt oss backa tiden till...

...för ett par hundra år sedan

- **Väldigt lokal och begränsad tillit**
 - Litade nästan bara på familj, släkt och närmaste grannar
- **Stark beroendeställning**
 - Samhället var mer ojämlikt - tillit var ofta kopplad till beroenden
- **Kyrkan och traditionen styrde**
 - Svenska kyrkan hade stor makt
 - Moral, heder och tillit var starkt kopplat till religion



I början av 1900-talet

- **Industrialisering**

- Folk flyttar till städer → möter fler okända människor → behov av ny sorts tillit

- **Folkrörelser**

- Organisationer växer fram som bygger tillit mellan främlingar
 - Facket, nykterhetsrörelsen, frikyrkor, Kooperation

- **Början på institutionell tillit**

- Regler
 - Organisationer
 - Avtal



Våra tillitsankare inför den digitala eran

- **Tillit främst genom**
 - Personliga möten
 - Fysisk närvaro i butiker, banker, myndigheter...
- **Vi litar på**
 - Människor vi träffat
 - Lokala institutioner
 - Etablerade auktoriteter som läkare, lärare, banktjänstemän...
- **I grunden långsamma, trygga och stabila system**



Analogt blir digitalt!

- **Tillit flyttar från människor till it-system**
 - Du måste lita på tekniken
- **Främlingar blir vardag**
 - Du interagerar med okända hela tiden
- **Snabbhet ersätter långsam kontroll**
 - Tillit måste skapas direkt
- **Plattformer ersätter institutioner**
 - Tilliten är inte alltid ömsesidig

Sammantaget stora utmaningar som måste övervinnas!

Finns det lärdomar från tidiga teknikkrig?

- **Fysiska nät- & länklagerkrig**

- ARCNET, Ethernet, Token Ring

- **Drivrutins- och stackkrig**

- NDIS (3Com, MS), ODI (Novell)

- **Protokollkrig**

- APPC/APPN, IPX/SPX, OSI, TCP/IP

- **Tillämpningskrig**

- SMTP, X.400

- X.400, SMTP

- **Tillämpningar**

- TCP/IP, OSI-modellen, IPX/SPX, APPC/APPN

- **Protokollkrig**

- NDIS (3Com, MS), ODI (Novell)

- **Drivrutins- och stackkrig**

- ARCNET, Ethernet, Token Ring

- **Fysiska nät & länklager**

Explosiv innovation → fragmentering → standardisering → dominans → acceptans

Vad är lärdomen?

- **Tre tillitsmodeller utmanades**
 - Företagskontrollerad tillit (ex 3com, IBM, MS, Novell) → Tillit = Varumärke + Kontroll
 - Institutionell tillit (ISO, ITU, "televerk") → Tillit = Byråkrati + Konsensus
 - Distribuerad tillit (IETF) → Tillit = Öppenhet + Fungerande implementation
- **80-talets teknikval var egentligen val av tillitsmodell och utgör tillika grunden för internet där receptet förenklat är:**
 - Distribuerad, öppen och verifierbar men ofullständig och med adaptiv tillit

Tänk även på detta när ni väljer IoT-lösningar, molntjänster, AI-modeller...

Vad utgör tilliten till internet?

- **Tekniken är inte fulländad – vilket också är internets framgång!**
- **Institutionell styrning**
 - ICANN – Global multistakeholders → Tillit = Konsensus + Organisatorisk legitimitet
 - IANA IP-adressering, AS, rotzonen → Tillit = Korrekthet + Konsistent över tid
 - IETF – Standardisering (RFC:er) → Tillit = Transparens + Fungerande implementation
- **Tre olika organisationer i tre olika roller → Uppdelad tillit**
 - Du litar fortfarande på root-DNS – Numera med ett extra lager tillit i form av DNSSEC
 - Du litar på att dessa organisationer inte kapas och på att stater inte tar över dem

Större behov av ömsesidig tillit

- **Internet fyller sitt syfte men löser långt från alla tillitsfrågor**
 - Internet löser transportering och adressering
- **Tillämpningarna måste ytterst axla tillitsutmaningarna**
 - Kan lösas med nya lager av infrastrukturella tilläggsfunktioner för tillit
- **Det innebär fler tillitsankare, som också behöver få acceptans**
 - Rom byggdes heller inte över en dag
- **Tillitsankare med matematisk tillit i form av asymmetrisk kryptografi**
 - Med "ännu större" inslag av organisatorisk legitimitet och styrning

Det blir tyvärr ofta en ensidig syn på tillit...

Tillitstermometern

- **Det är inte perfekt, men vi har kommit längre än vad vi tror**
 - Vi var tidiga med tillitsramverk för e-legitimationer och federationer (2010)
 - Bra utbud med granskade och godkända e-legitimationer och e-tjänstelegitimationer
- **Vi linjerar sämre med eIDAS än önskvärt**
 - Vi är sena med kvalificerade elektroniska underskrifter
 - Vi är sena med e-leg på tillitsnivå 4 och den digitala plånboken
 - Vi är sena med att använda QWAC-cert (Steria/Expisoft lever gott 😊)
- **Utanför EU äger vi inte spelreglerna**
 - De amerikanska aktörerna, med proprietära lösningar, dominerar marknaden

Ett tunt lager infrastruktur för tillit

- **Exemplet identitetsfederationer**
 - Identitetsfederationer har i praktiken funnits i +15 år
- **Federationsoperatören ansvarar för regelverk och teknik (=tillit)**
 - E-legitimationsutfärdare och e-tjänsteleverantörer accepterar tillitsramverk och tekniskt ramverk vilket innebär att de också litar på varandra (kryptografiskt och organisatoriskt)
 - I Sverige granskar och godkänner Digg e-leg vilket förenklar för federationerna
- **Inom utbildningssektor är federationer självklara (Skolfederation & Sunet)**
- **Trots framgång finns det centralistiska hinder**
 - Flera organisationer föredrar att bara lita på sitt eget ekosystem och låta det ekosystemet integreras med enskilda e-tjänster, API:er etc där behov uppstår

Tillitsbarometern

- **Tillit till DNS – Klart, men allt för många i hängmattan**
 - DNSsec (IANA/ICANN)
- **Tillit till kvalificerade betrodda tjänster (eIDAS) – Stackmoln**
 - Underskrifter, e-leg, webbplatser, API:er (EU trustlist)
- **Tillit till web (https), mejl (S/MIME), api:er (mTLS), tid (NTPS) – Orosmoln**
 - Ofta listor i operativsystem och webbläsare över pålitliga utfärdare (CA/B Forum)
 - Detta är en oerhört brokig terräng där tillitsfrågan inte alltid är självklar
- **Proprietära tjänster – Oönskade**
 - Underskrifter (Adobe)

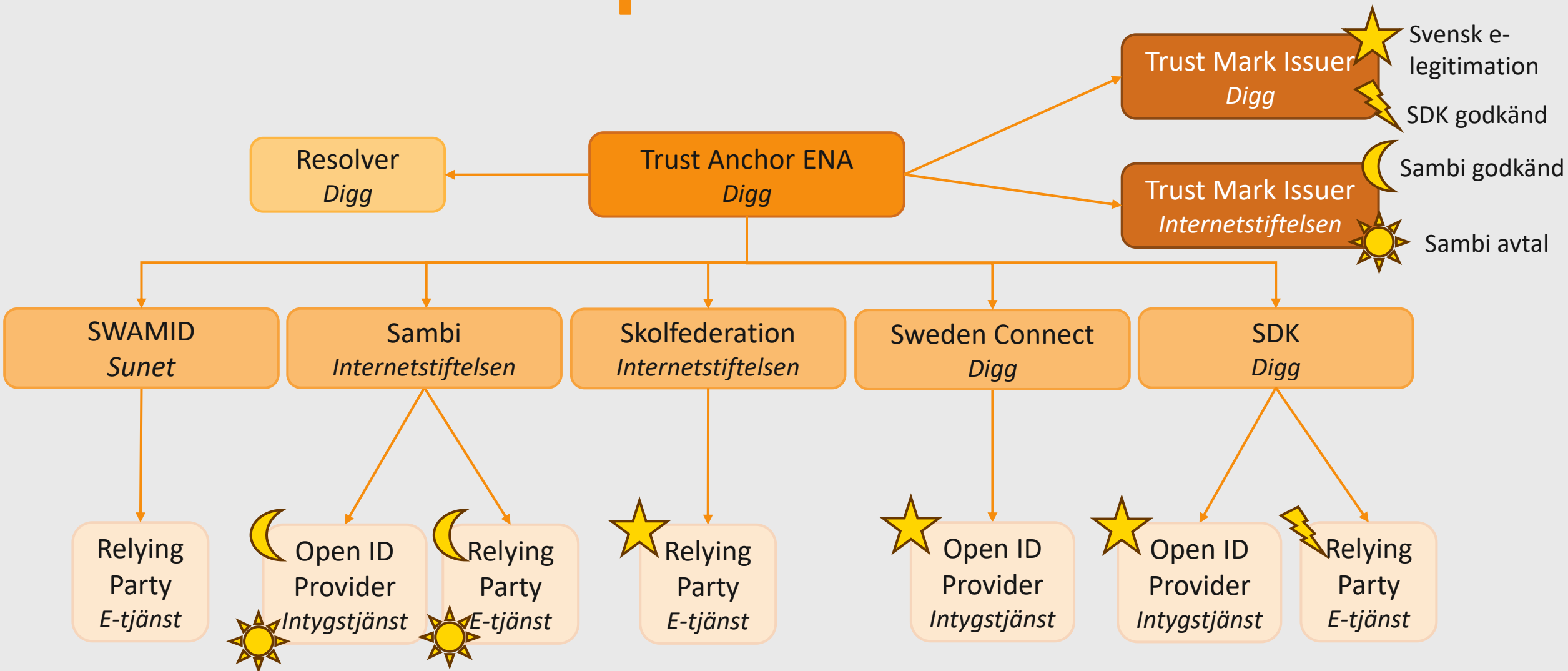
Det finns bra ambitioner

- **Tre förslag som vuxit fram över tid**
 - Diggs förslag om en sammanhållen infrastruktur för identitet & behörighet (2025)
 - SKR:s rekommendation för identitet & behörighet (2025)
 - Ineras referensarkitektur för identitet & åtkomst (2023)
- **Är Diggs förslag för komplicerat bitvis?**
 - Tillit = Konsensus + Organisatorisk legitimitet?
 - Tillit = Byråkrati + Konsensus?
 - Tillit = Varumärke + Kontroll?

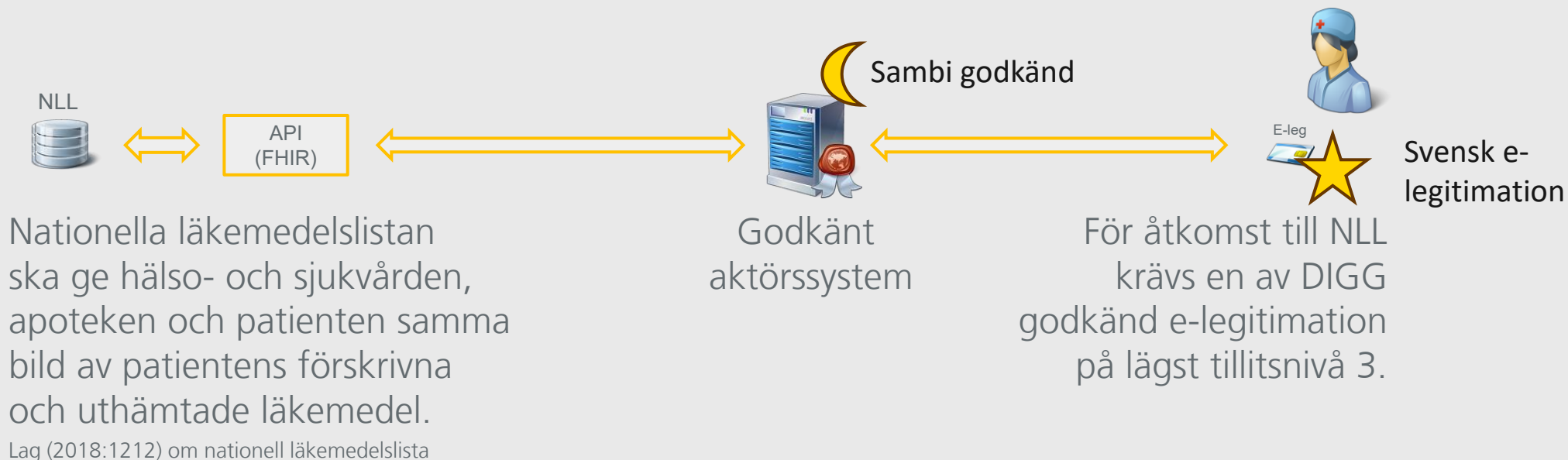


Samtidigt är det långt bättre än att blunda och kasta lösenordshashar västerut

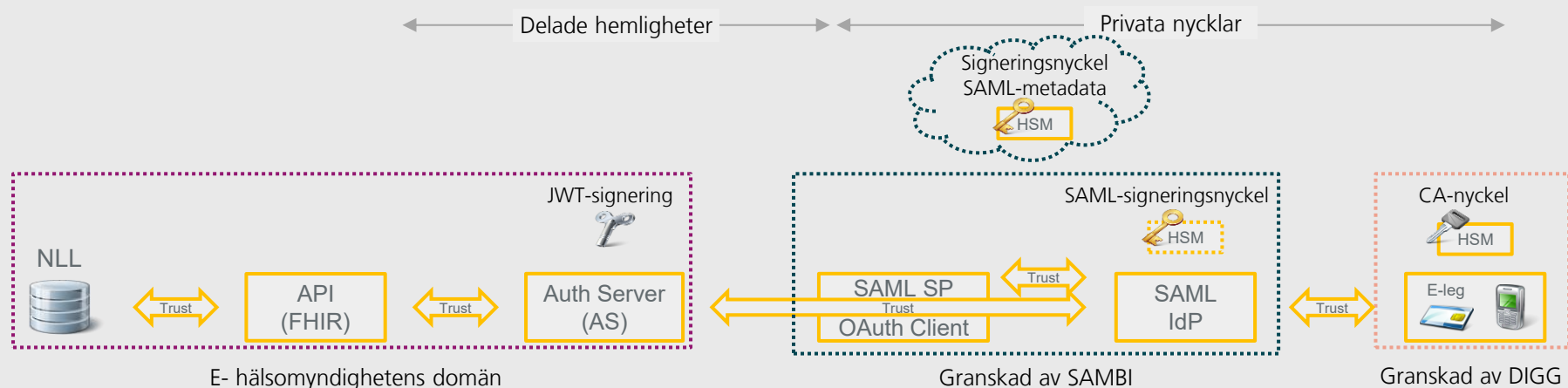
Framtida ENA OpenID Connect federation



Tillitskedjan till NLL som exempel med ENA



Tillitskedja till NLL via Sambi utan ENA



E-hälsomyndighetens Handbok för vård- och apotekstjänster – [Intygsväxling - OAuth2 token service](#)

The OAuth 2.0 Authorization Framework [[RFC6749](#)]

Security Assertion Markup Language (SAML) 2.0 Profile for OAuth 2.0 Client Authentication and Authorization Grants [[RFC7522](#)]

SAML-intyget **MÅSTE** innehålla <Conditions> element med ett <AudienceRestriction> element med ett <Audience> element som identifierar Auktorisations Servern som målgrupp. Detta <Audience> element FÅR beskrivas som en URI med Auktorisations Servers token endpoint URL. Auktorisations Servern **MÅSTE** avvisa SAML-intyg som inte innehåller sin egen identitet som målgrupp. [RFC7522.3.2]

JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants [[RFC7523](#)]

Summaring

- **Innovation → fragmentering → standardisering → dominans → acceptans**
 - Det är stora inslag av ofrivillig acceptans
- **Det finns trots allt en hel del av tillitsvärden inom ramen för eIDAS2**
 - I Sverige har eIDAS-aptiten varit låg
- **Statlig e-legitimation och plånboken är viktiga steg**
 - Rörelsen mot tillitsnivå 4 är tydlig
- **En hel del tillit är inte ömsesidig – Ska vi fortsätta att acceptera det?**
 - Plattformsleverantörerna sätter spelreglerna utifrån sina behov

Det är en utmaning kvar som vi inte berört...

Dagens matematiska tillit i farozonen

- **Dagens asymmetriska algoritmer är utdömda**
 - Exempelvis RSA från 1975
 - Tidtabellen när de riskerar att knäckas är ett par år till ett par decennier
- **Stor oro för "Harvest now, decrypt later"**
- **NIST annonserade 2024 tre kvantdator säkra algoritmer (PQC)**
 - Ytterligare algoritmer är på väg
 - Kräver förändringar i både mjukvara och hårdvara (HSM, IoT, smarta kort, TPM)
- **Påbörja inventeringen av hur ni använder asymmetrisk kryptografi**
 - CBOM - Cryptographic bill of materials

<https://certezza.net/uncategorized/vagledning-vid-migrering-till-kvantdatorsakra-algoritmer/> (2025-05-06)



TACK!

Thomas Nilsson
thomas@certezza.net

30-årsfirande 1:a december på Oscars
Se <https://sakerhetsdagen.se/>