



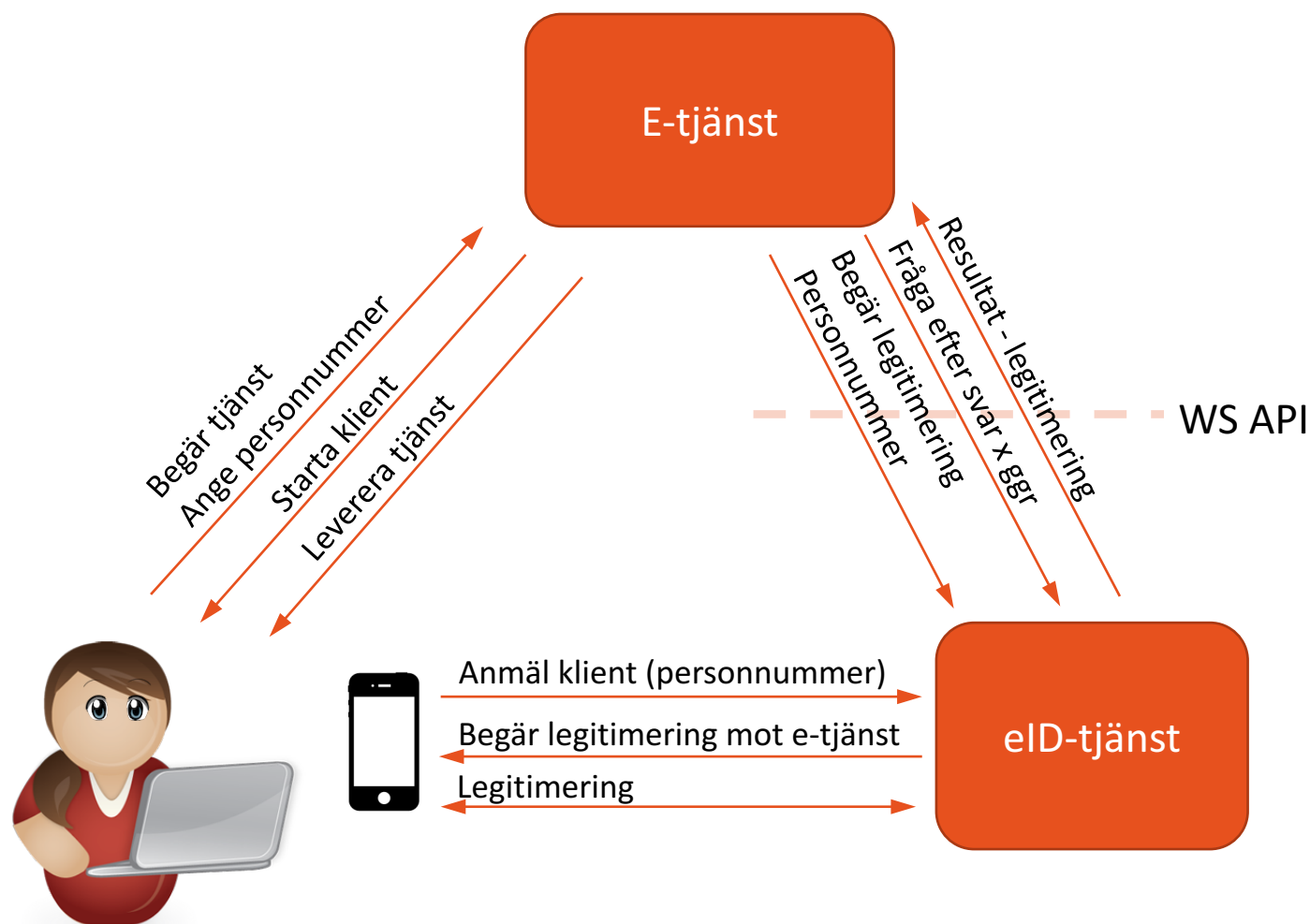
E-LEGITIMATIONS NÄMNDEN

Introduktion till SAML federation

Varför använda SAML federation för elektronisk legitimering och underskrift

Stefan Santesson
Martin Lindström

Integration med befintlig eID infrastruktur (Typfall)



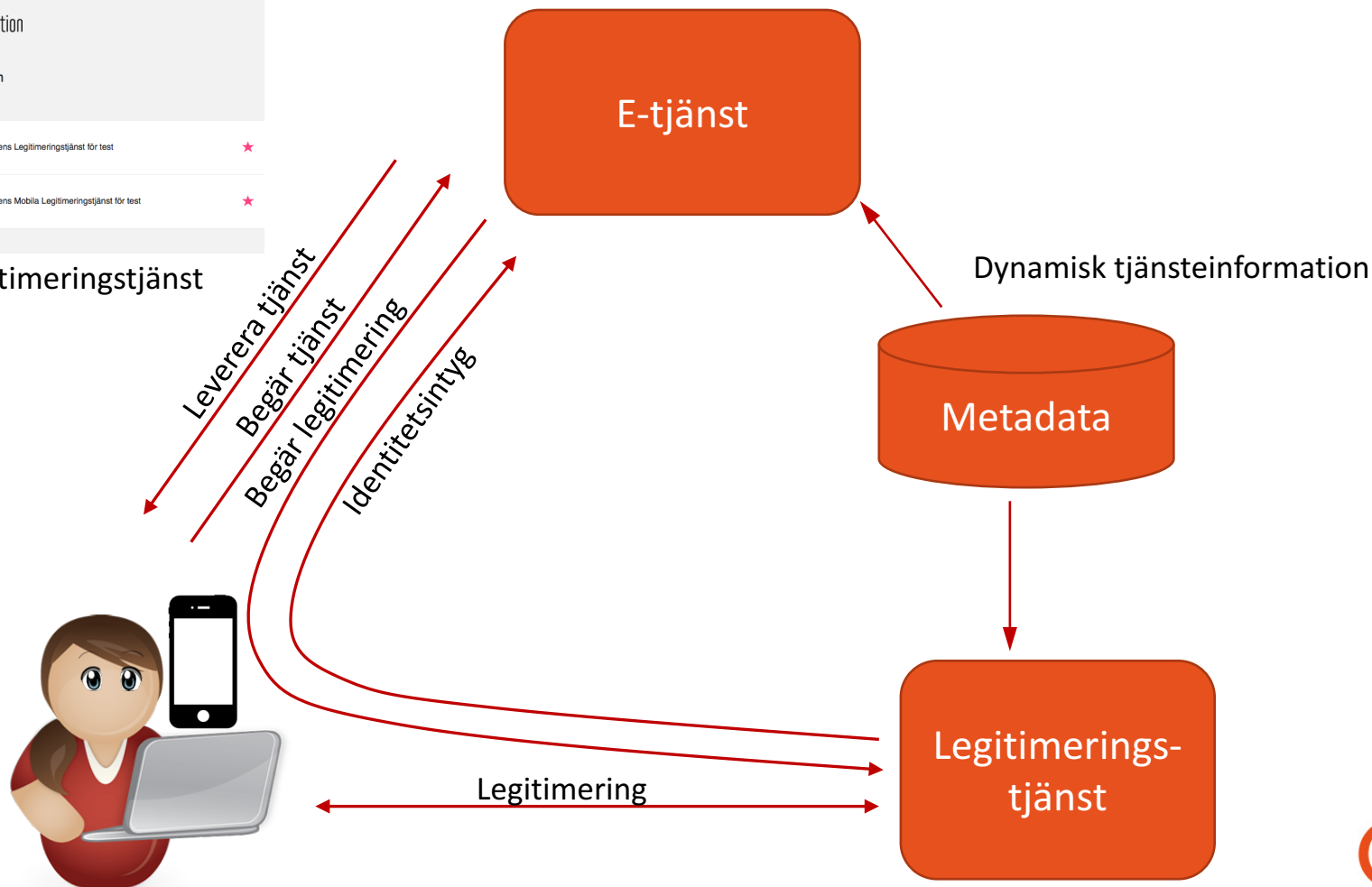
Utmaningar – traditionell integration

- Inget standardiserat gränssnitt
 - Kommunikation med eID server
 - Starta klient
 - Konsumera identitetsuppgifter
- Unik integration mot varje eID-tjänst.
- Kräver aktiv och upprepad förfrågan efter resultat
- Ej automatisk tillgång till nya eID tjänster.
- Anvisningstjänst/användargränssnitt
- Bindning – Användarsession mot legitimering
- Sessionshantering
- eID specifik integration av underskrift
- PKI-baserad klient – statiska certifikat
- Ej öppen valideringslösning för underskrifter
- Integration mot eIDAS (Svensk e-legitimation underlättar)

Legitimering (SAML) – Svensk e-legitimation



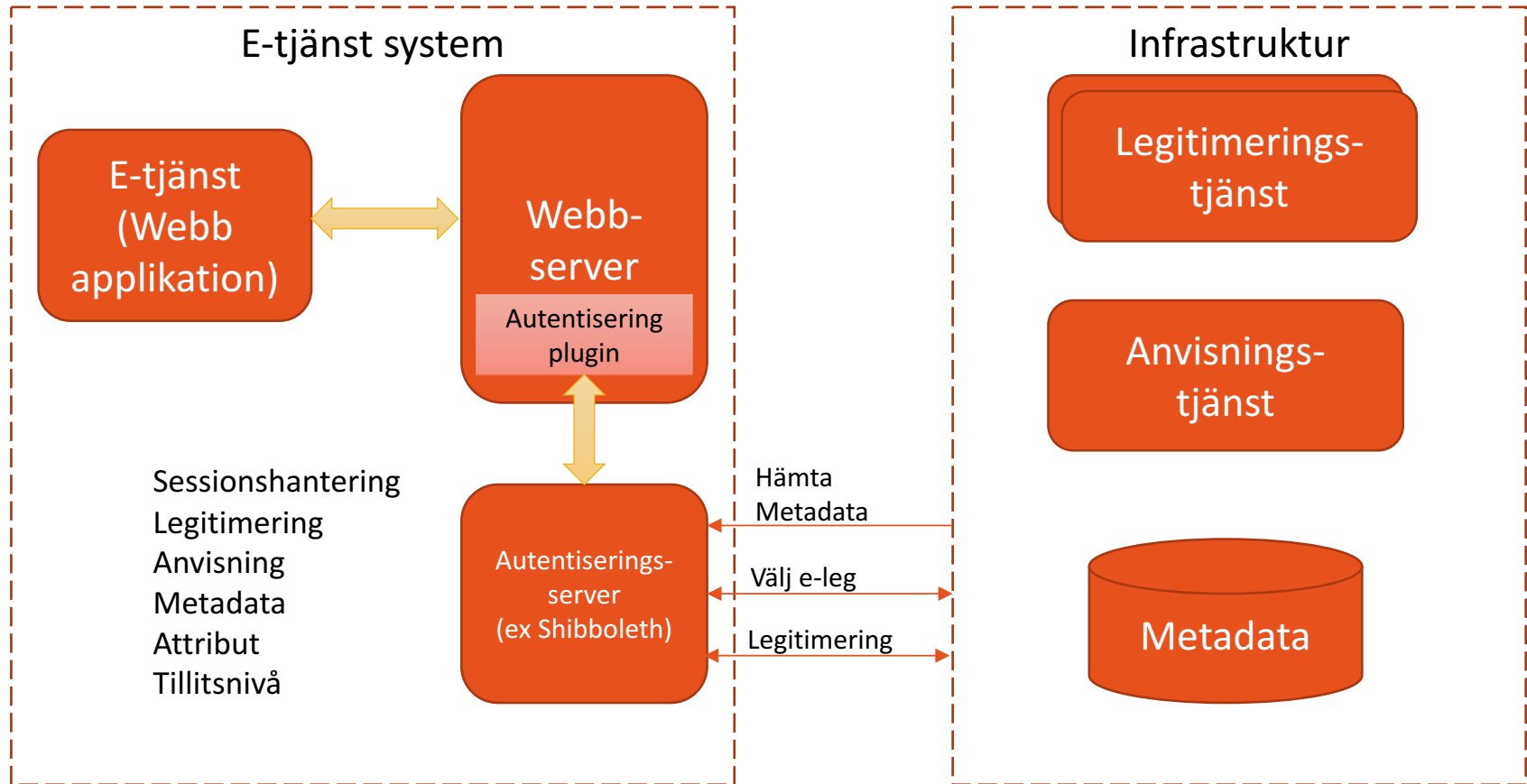
Välj Legitimeringstjänst



Legitimering med SAML

- Standardiserat gränssnitt
- En integration mot alla legitimeringstjänster
- Starkare bindning av e-tjänstklient
- Dynamisk anvisning/användargränssnitt vid val av e-legitimation
- Dynamisk konfiguration via metadata
- Integration med underskriftstjänster
- Enkel integration mot eIDAS

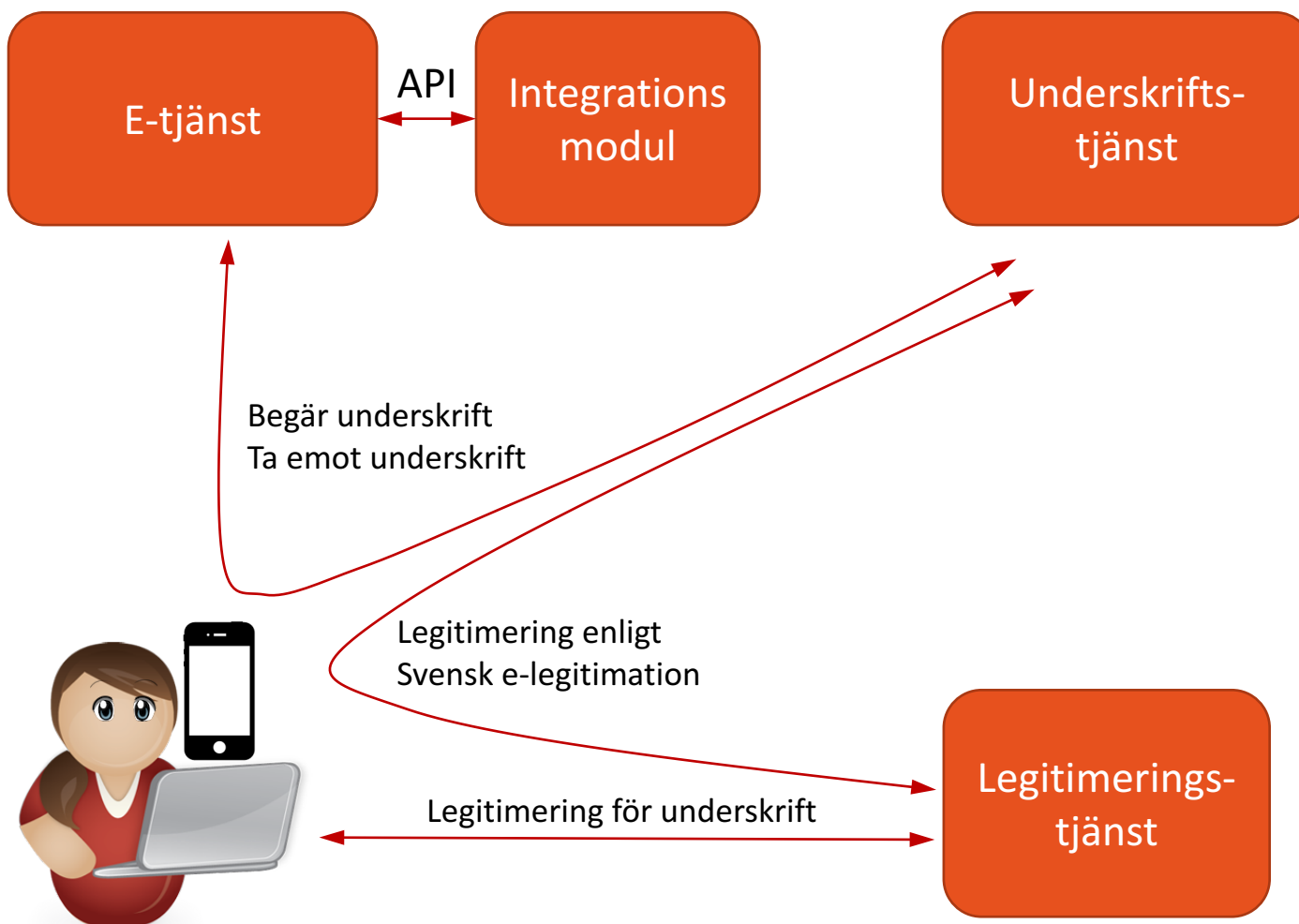
Typisk SAML integration



Typisk SAML integration

- Autentiseringsserver
 - Standard produkter eller Open Source
 - Hanterar all SAML (Request, Response, Metadata)
 - Sessionshantering
 - Levererar attribut med varje http request till skyddad tjänst
- Anvisning
 - Bestäm integrationsmetod
 - Anpassning av webbsidor för inloggning
- Webbserver
 - Aktivera modul för SAML autentisering
 - Definiera resurser som kräver SAML autentisering
 - Ta emot attribut (http/ajp request attribut) och information om legitimering (Legitimeringstjänst, Tillitsnivå etc).

Integration med underskriftstjänst




Integration med underskriftstjänst

E-LEGITIMATIONS NÄMNDEN

E-legitimationsnämndens Legitimeringstjänst för test

Din underskrift har begärts av


SP Myndighetens Signatortjänst
Testmyndighet underskriftstjänst för test

Information om vad som undertecknas

You are requested to sign the following document:

Document name 5da8949a1a462c243fbc69906a9edf7.xml
Signer name Clarence Hammarström
Signer ID personalIdentityNumber: 198907028412

Clarence Hammarström (198907028412)

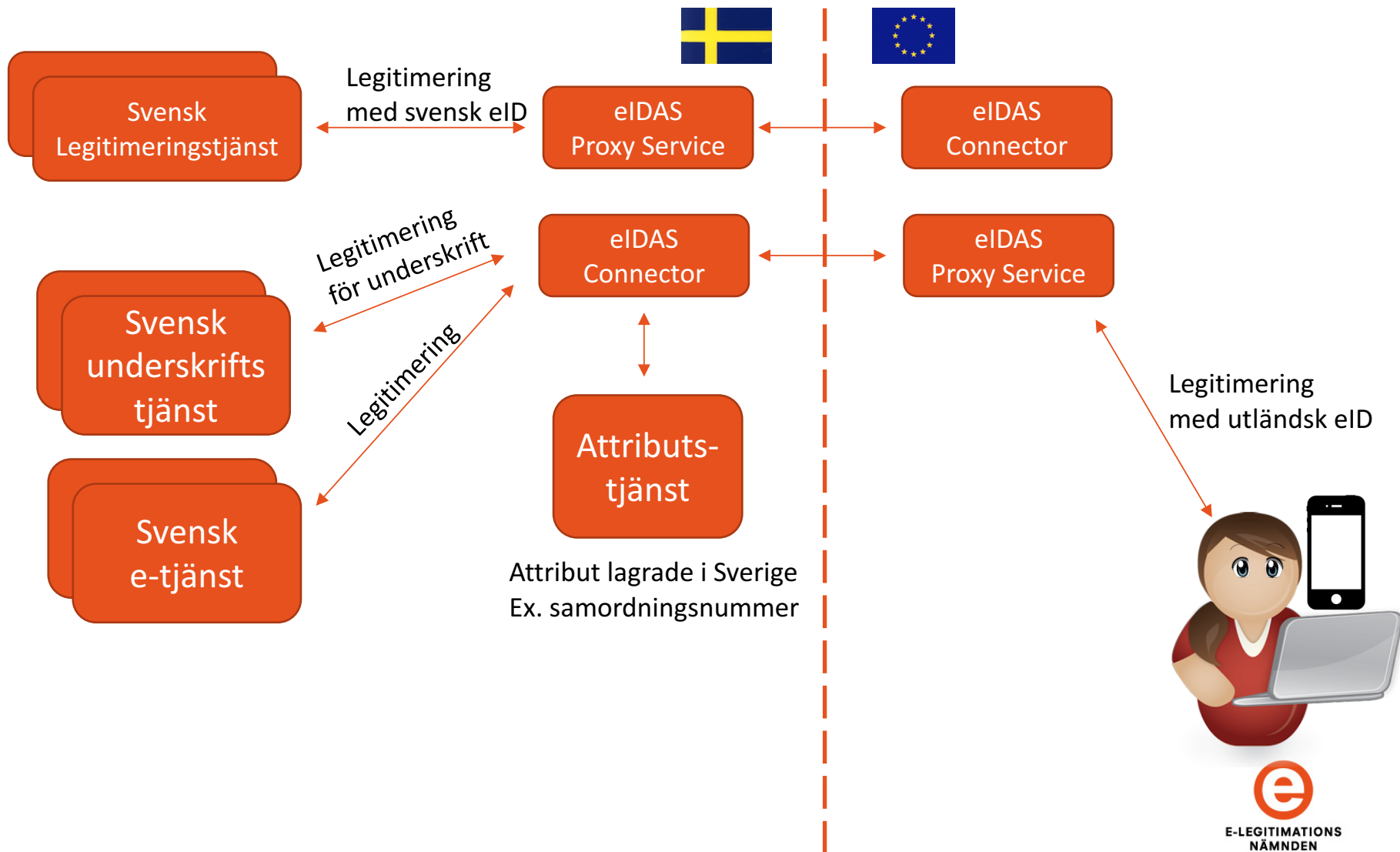
Användar ID

Lösenord

Integration mot underskriftstjänst

- Integrationstjänst skapar sign request enligt OASIS DSS standarden, samt hanterar response.
- Dokument som signeras lämnar aldrig e-tjänsten
- Krypterat underskriftsmeddelande till legitimeringstjänsten
- Legitimeringstjänster har anpassat gränssnitt för underskrift
- Kompatibelt med legitimering från eIDAS noder. Möjliggör underskrift med utländsk eID.

Integration mot eIDAS (Under utredning)



Integration mot eIDAS

- E-tjänst begär legitimering enligt Svensk e-legitimation
- Utökad attributsprofil
- Möjlighet att knyta svenska ID attribut till utländsk eID, ex personnummer och samordningsnummer.
- Hantering av eIDAS policy
 - eIDAS tillitsramverk
 - Notifierade eID
- Integration med signeringstjänst ger stora fördelar. Problemet fortfarande olöst vid underskrift i ursprungsland.
- Kräver underskrifter som kan valideras öppet och gratis.