CERTEZZA

Lååååånga kedjor av tillit

Thomas Nilsson
thomas@certezza.net

Att notera…

- Jag exemplifierar med E-hälsomyndighetens nya säkerhetslösning för åtkomst till Nationella läkemedelslistans (NLL) API
  - Jag använder exemplet i syfte att visa på allt längre tillitskedjor och i ett LoA3 perspektiv
  - Jag har ingen åsikt om lösningsvalet i sig utan ser det som en naturlig utveckling i brist på andra ekosystem
- Detta är inte ett uttömmande exempel

Åtkomst till NLL

Nationella läkemedelslistan ska ge hälso- och sjukvården, apoteken och patienten samma bild av patientens förskrivna och uthämtade läkemedel.

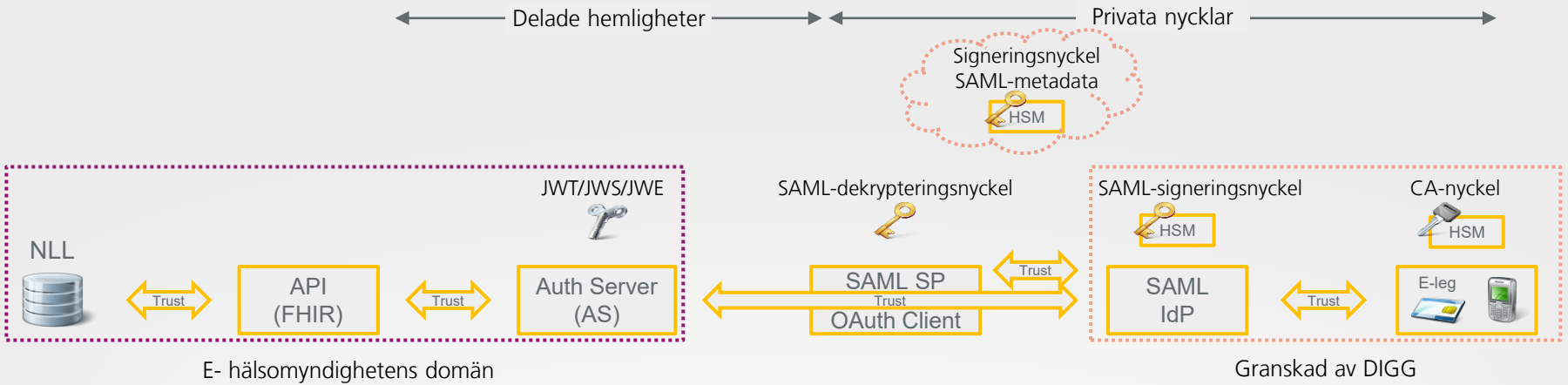
Lag (2018:1212) om nationell läkemedelslista

Aktörssystem

För åtkomst till NLL krävs en av DIGG godkänd e-legitimation på lägst tillitsnivå 3.

CERTEZZA

Tillitskedjan NLL – Sweden Connect



E-hälsomyndighetens Handbok för vård- och apotekstjänster – Intygsväxling - OAuth2 token service

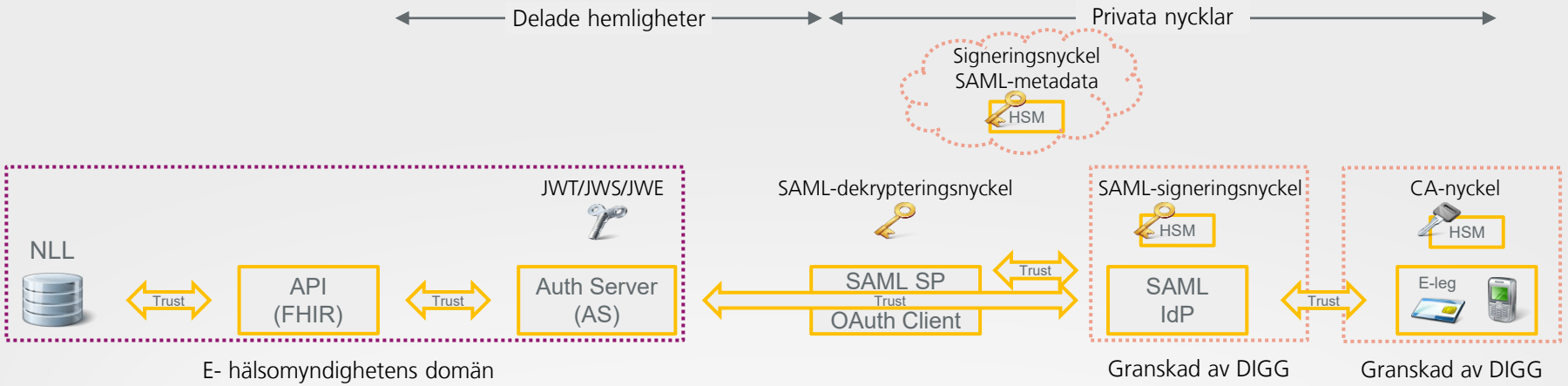
The OAuth 2.0 Authorization Framework [RFC6749]

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 Serverns token endpoint URL. Auktorisations Servern **MÅSTE** avvisa SAML-intyg som inte nnehåller sin egen identitet som målgrupp. [RFC7522.3.2]

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

Tillitskedjan NLL – Sweden Connect



E-hälsomyndighetens Handbok för vård- och apotekstjänster – Intygsväxling - OAuth2 token service

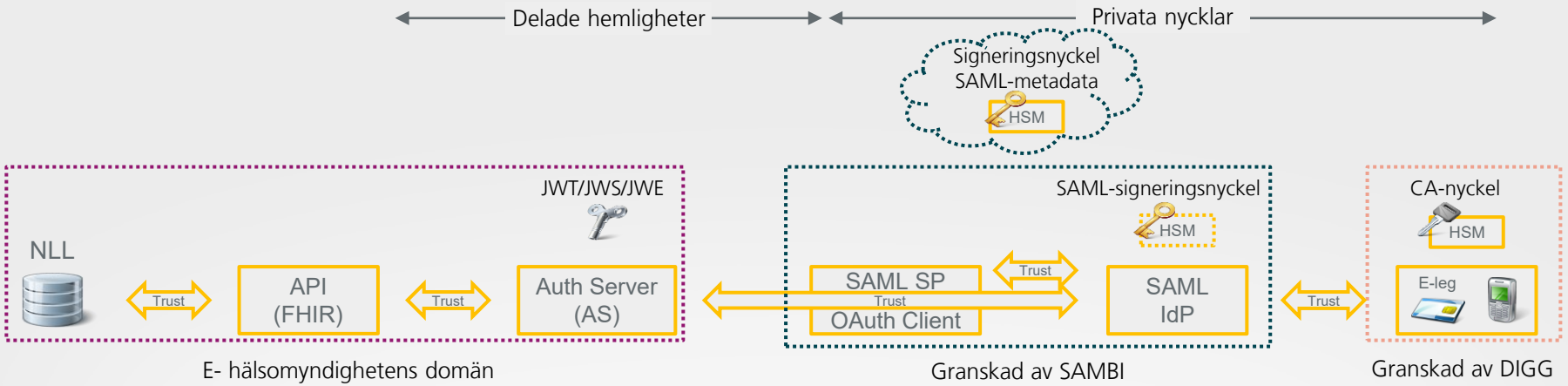
The OAuth 2.0 Authorization Framework [RFC6749]

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 Serverns token endpoint URL. Auktorisations Servern **MÅSTE** avvisa SAML-intyg som inte nnehåller sin egen identitet som målgrupp. [RFC7522.3.2]

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

Tillitskedjan NLL – Sambi



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 Serverns token endpoint URL. Auktorisations Servern **MÅSTE** avvisa SAML-intyg som inte nnehåller sin egen identitet som målgrupp. [RFC7522.3.2]

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

CERTEZZA

OIDC federation ger sannolikt

- nya utmaningar, men den ger också,
- kortare tillitskedjor,
- bredare marknadsacceptans,
- förenklade klientimplementationer, och
- ett rikare ekosystem med fler aktörer!

CERTEZZA