Swedish eSENS Architecture

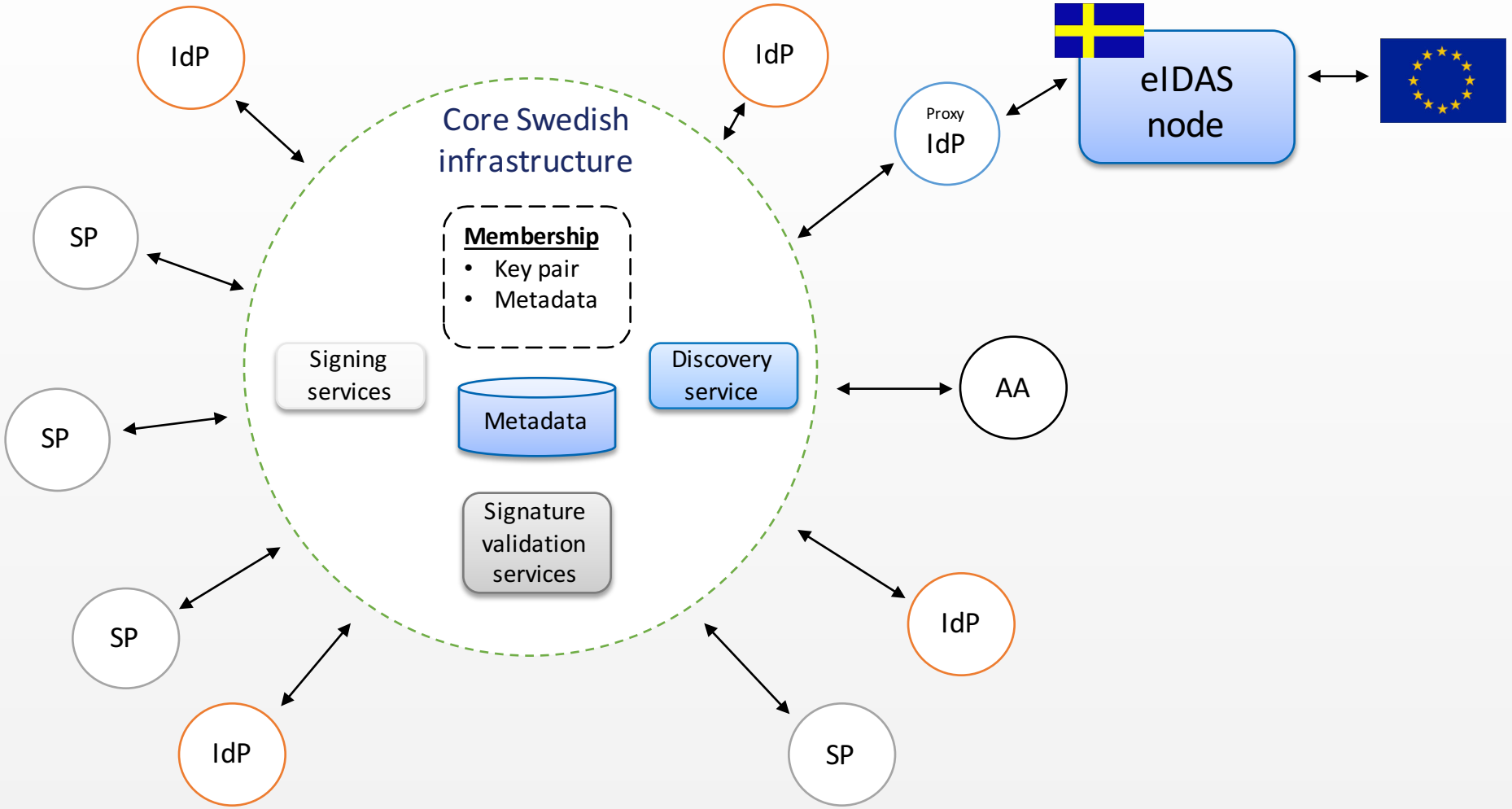
Cross-Border Authentication and electronic signing

using the Swedish eSENS infrastucture

Swedish eSENS pilot infrastructure

- Connects European citizens to Swedish government e-Services
- Allows users to authenticate their identity and sign documents using their national eID.
- Only requires cross-border authentication.
- Fully implemented demo infrastructure fully operational today. Implementing both cross-border authentication and signing.
- Easy to integrate into Service Providers. Subscribing to the Swedish national eID infrastructure includes integration with Europe citizen eID:s with no additional work.
- Cross-border integration complexity off-loaded to national proxy service

Swedish eSENS Pilot Architecture



Roles

Role	Description
SP	Service Providers, providing electronic services to Swedish and European citizens
IdP	Identity Providers, providing means to authenticate users
AA	Attribute Authorities, providing additional attributes about users
eIDAS node	Routes authentication requests to eID services in other European countries, allowing users to authenticate using their national eID.
Signing Service	A service providing the capability to sign electronic documents to any user that can authenticate their identity.
Signature Validation Service	A centralized service with extended capability to validate different types of signatures based on national and European trust information.
Metadata	Information about services required to allow services to exchange data securely.
Discovery Service	Provides a generic UI where users can select a suitable IdP

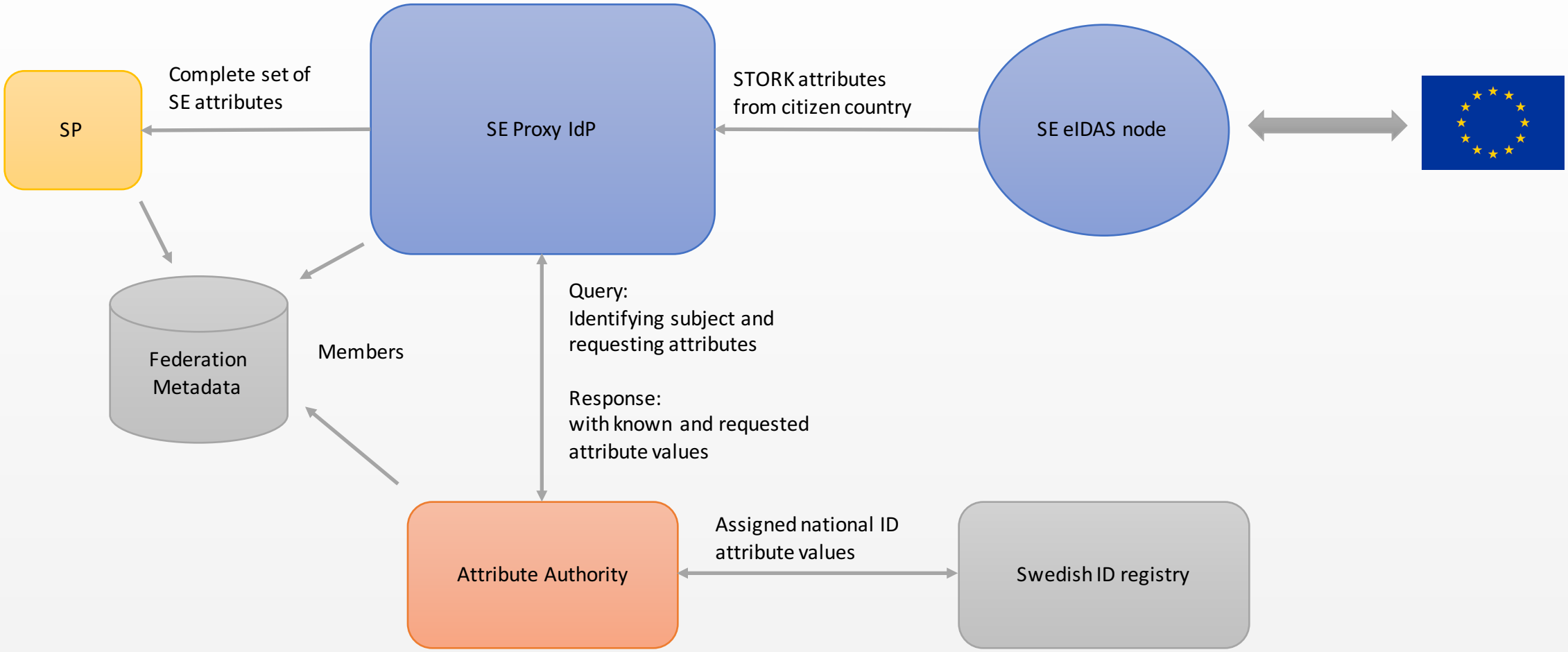
Basic Authentication Flow

- User requests a restricted service
- User selects an IdP consistent with the user's eID.
- User is transferred to the IdP for authentication.
- User is authenticated
- The IdP returns the user to the SP with a signed identity assertion holding data about the users identity
- The SP grants/denies access to the restricted service.

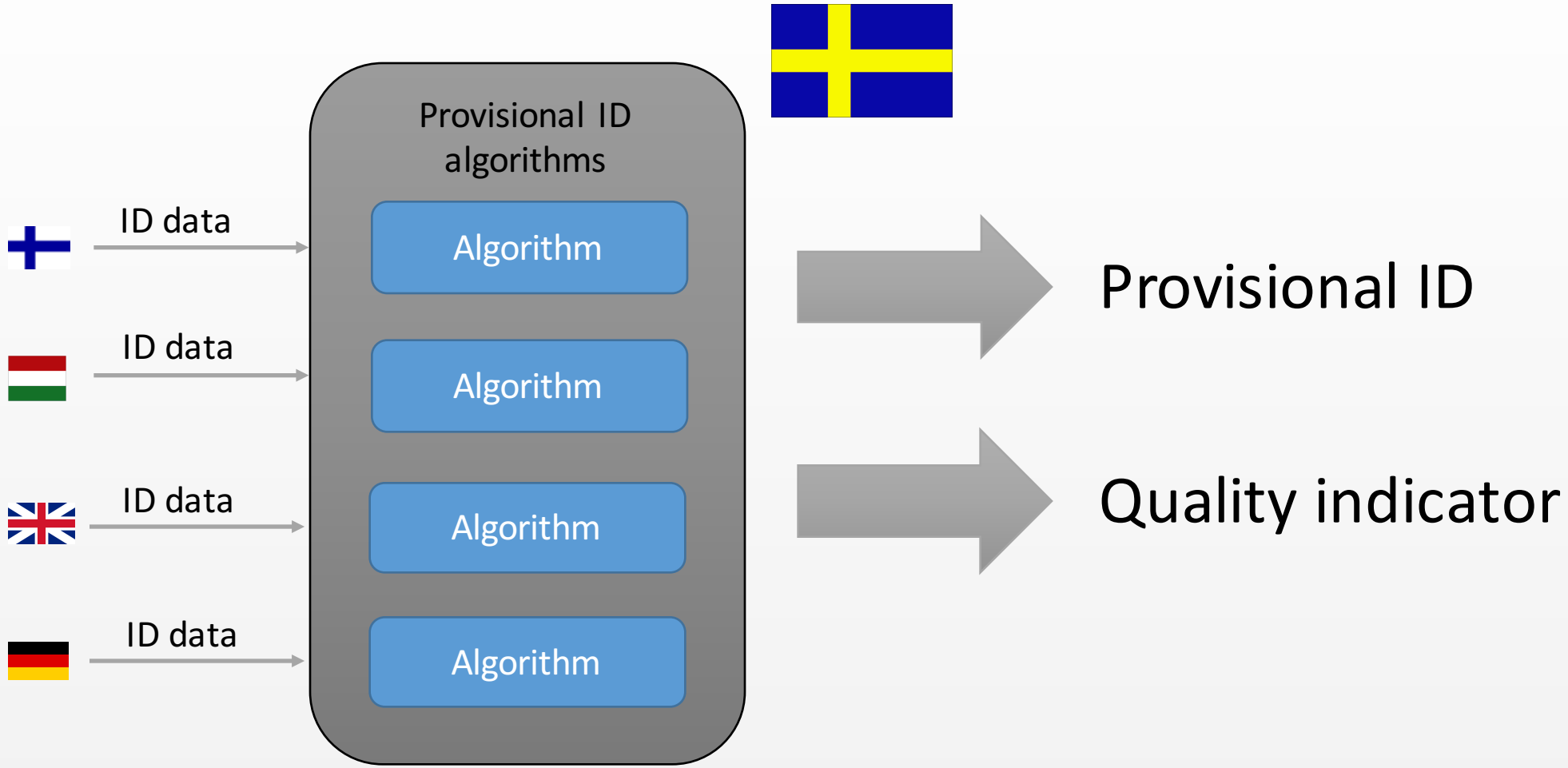
Obtaining relevant identity data

- Service providers need useful data about users through generic and country independent syntax and semantics.
- Service providers can’t do unique integration for each citizen country.
- An Attribute Authority expands the attributes provided about European citizens to Swedish Service Providers with:
  - Provisional ID. A generic identifier generated from the identity data obtained from cross-border authentication.
  - Provisional ID quality. An indicator for the provisional ID’s resilience to change over time, rated as A, B or C.
  - Any Swedish national identifier (Swedish personal ID or Swedish co-ordination number) assigned to the authenticated person.

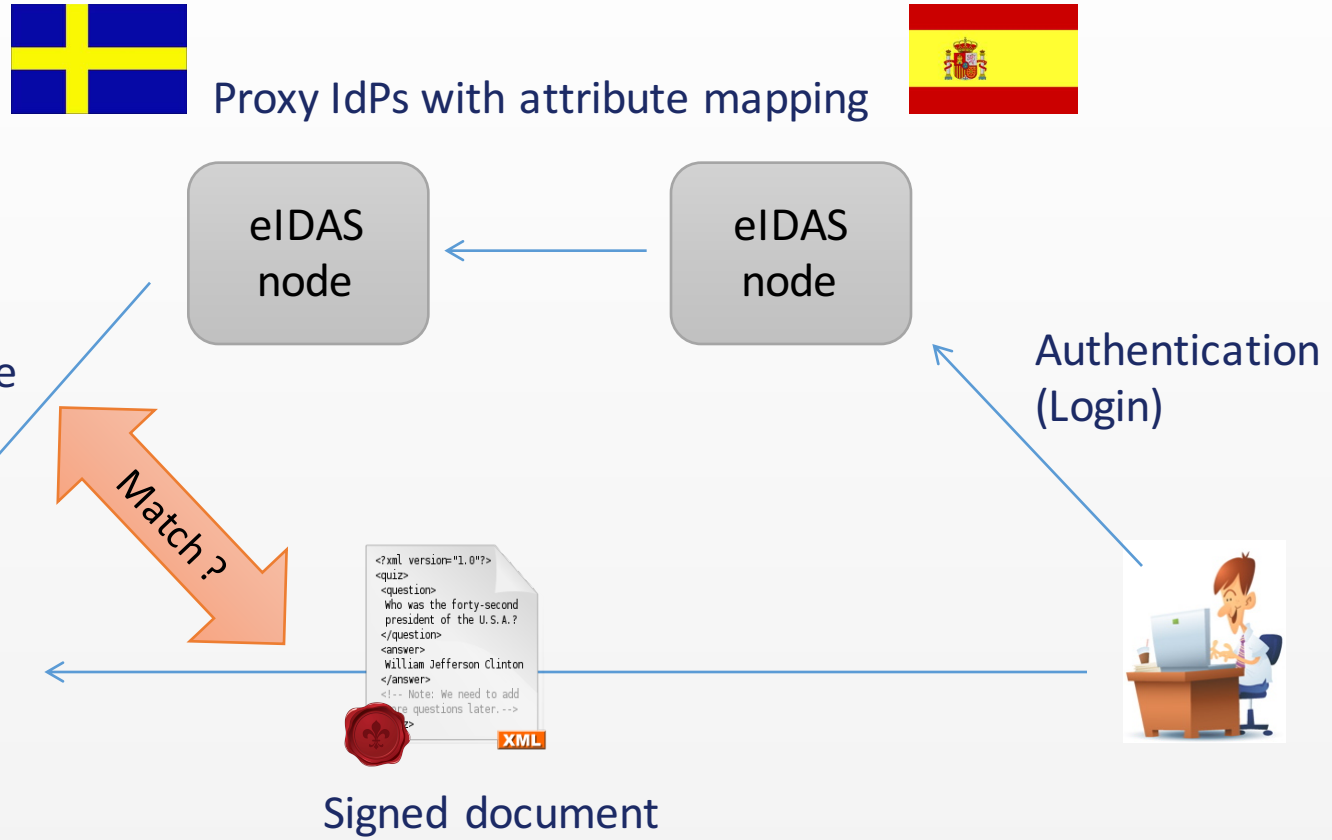
Attribute provider for national ID



The provisional ID
National attribute service



Did the right person sign?



Problem: Is the authenticated person also the signer?

The cross-border signing challenge

- Some eID:s do not provide the capability to sign a document.
- Having the user to sign a document locally in the citizen country introduces a wide range of problems for the service provider validating this signature in another country
  - Different signature formats
  - Determine trust in the signer's certificate
  - Obtaining useful identity information about the signer that may differ considerably from the identity data of the same person obtained through cross-border authentication.
  - Handling credential expiry and revocation status from other countries.

Federated signing

- Allows the user to sign documents using a signing service in the service provider country.
- Solves many practical problems
  - Always the same signature format
  - No time-stamping needed (Signature certificate issued at the time of signing).
  - Always the same validity period
  - Better user integrity. The document to be signed never leaves the service provider.
  - Almost no need for certificate revocation
  - The user identity in the signature certificate is consistent with the same user's identity through cross-border authentication
  - All types of eID:s can be used, also eID:s with no signing capability.
  - New information flow with signature accept and proof of sign message display and accept ensures that the user is aware that a document is being signed.
  - WORKS TODAY – NO NEW STANDARDS ARE NECESSARY.

Basic Signing Flow

- The user examines the data to be signed in the e-Service and agrees to sign.
- The user is transferred to a signing service with a sign request.
- The sign service authenticates the user
- The authenticated user is presented with information about what is being signed and accepts to sign.
- Signature key, signature certificate and signature data is generated and returned to the service provider.
- The service providers assembles the signed document.