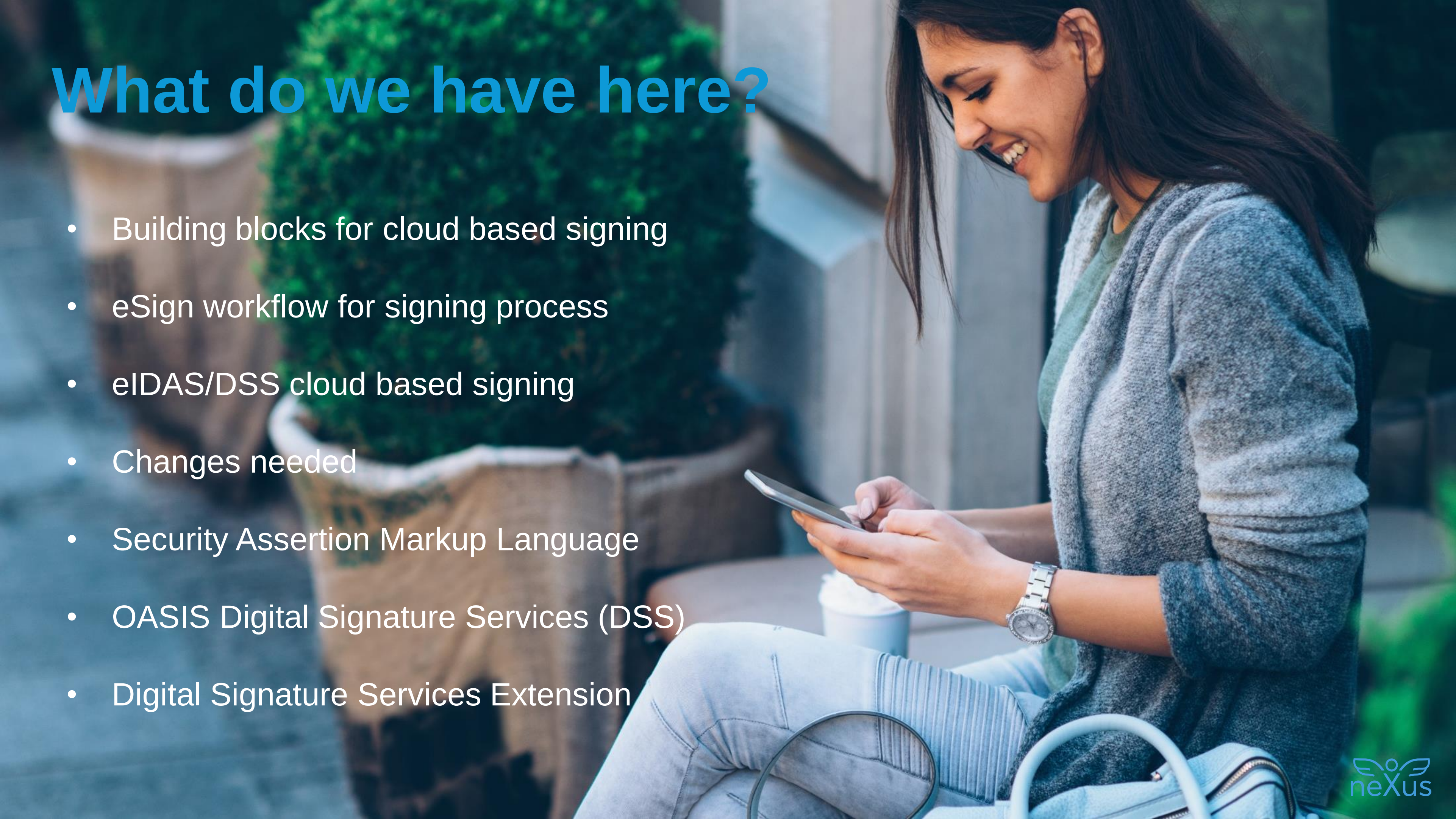
neXus

Enabling
trusted
identities

eSign convergence with global standards eIDAS/DSS

Manish Soni

16-11-2017



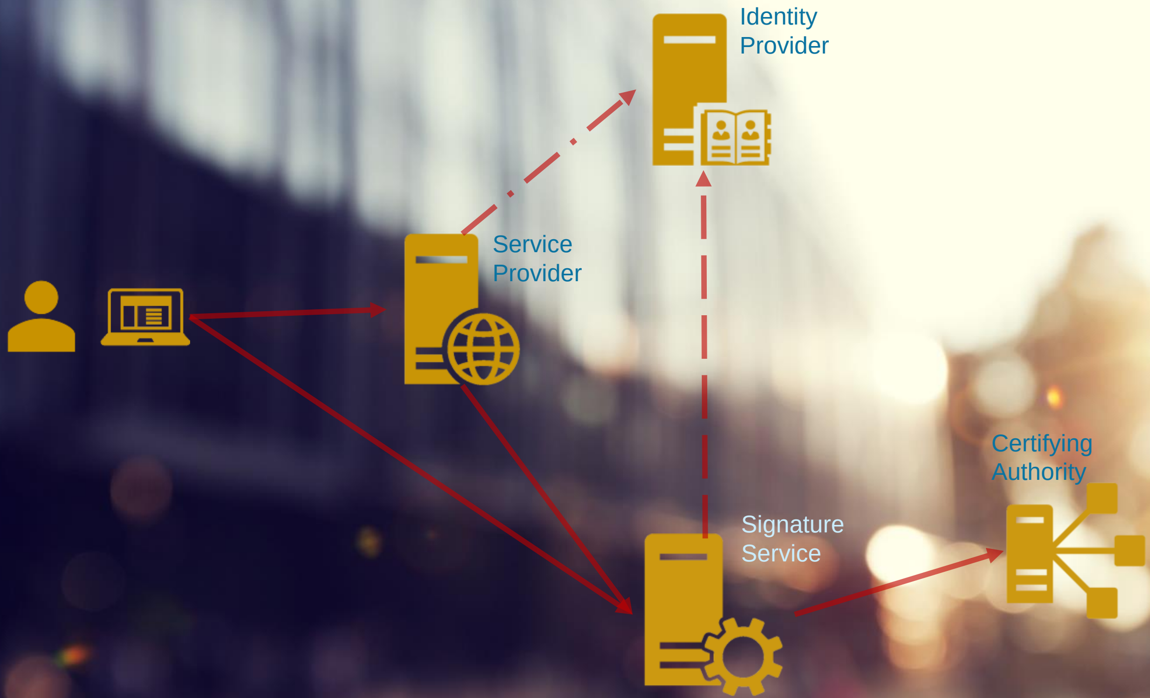
What do we have here?

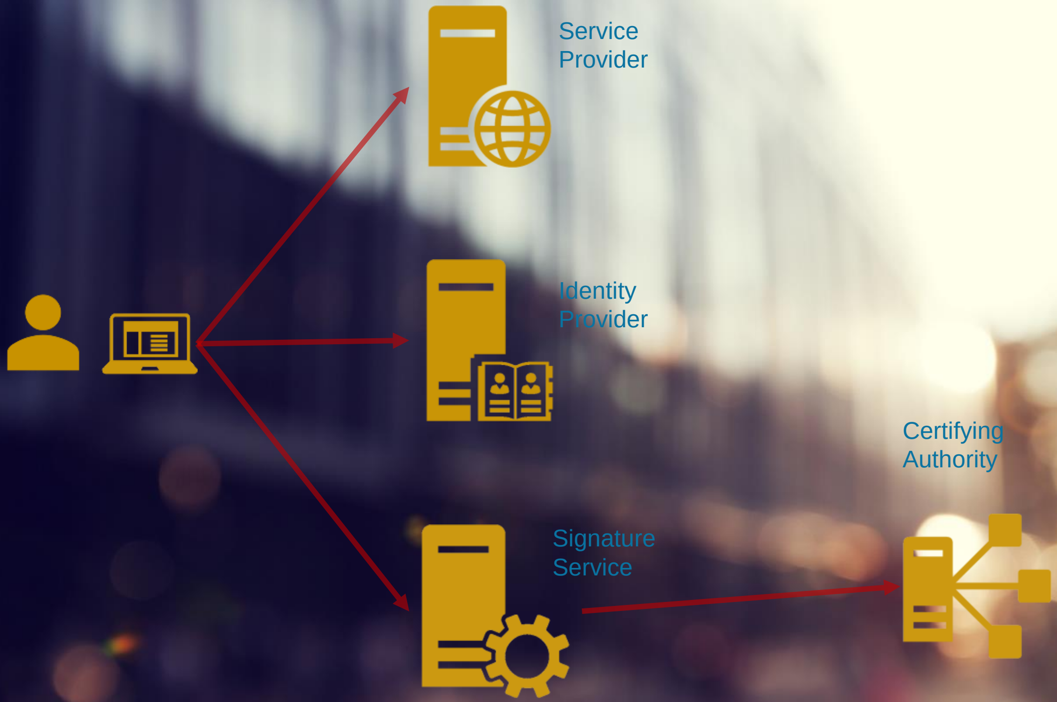
- Building blocks for cloud based signing
- eSign workflow for signing process
- eIDAS/DSS cloud based signing
- Changes needed
- Security Assertion Markup Language
- OASIS Digital Signature Services (DSS)
- Digital Signature Services Extension

- User
- Service Provider
- Signature Service
- Identity Provider
- Certifying Authority

Building blocks for cloud based signing

eSign workflow for signing





eIDAS/DSS cloud based signing

neXus

Changes needed

- SAML Identity Provider over UIDAI API.
- DSS as a framework.
- DSS extensions to incorporate SAML and other compliance information.

Security Assertion Markup Language

- SAML 2.0 became an OASIS Standard in March 2005
- Three types of statements are provided by SAML:
  1. Authentication statements
  2. Attribute statements
  3. Authorization decision statements

- https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language

OASIS Digital Signature Services (DSS)

- SignRequest message has two different parts
  - InputDocuments: This element contains information on the documents that must be signed
  - OptionalInputs: The core document defines contents profile.
- The SignResponse message has three relevant parts
  - Result: with details of the result of the server's operation
  - SignatureObject: which may enclose the signature created
  - OptionalOutputs

Digital Signature Services Extension

- SignRequestExtension: is used to supply essential sign request information to a DSS Sign request.
  - <saml:Conditions>
  - <IdentityProvider> The SAML EntityID of the Identity Provider is used to authenticate the signer before signing
  - <SignMessage> [Optional] provides a html encoded message to the signer

Thank you!

Manish Soni
manish.soni@nexusgroup.com
+91-9225242123

neXus | Enabling trusted identities

nexusgroup.com