SAML 2.0 - Work Item 5a
Liberty Enabled Client or Proxy (LECP)

Frederick Hirsch

Nokia Mobile Phones

03-09-08

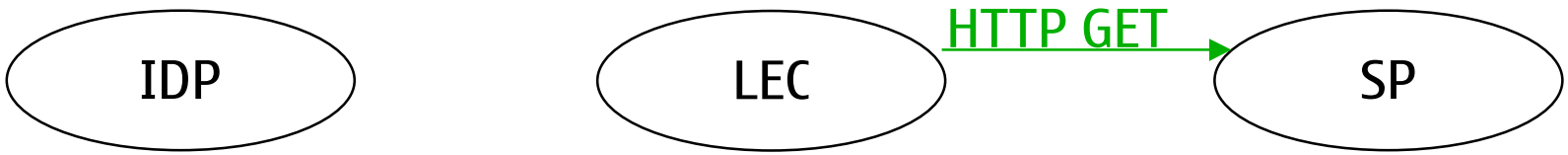
NOKIA

LECP: Concepts

- Liberty Enabled Client or Proxy
  - knows or knows how to find appropriate IDP for principal + SP
  - Can follow the LECP profile and understand the schema elements
  - *It can deal with an authentication request from an SP*
- Benefits
  - Simple - no redirects, no cookies
  - Avoids performance issues of redirects in certain deployments
  - Supports cross-business deployments with multiple IDPs
  - Simple SP can support it
  - LEC can check correctness
  - Allows simple clients to be configured to allow authenticated access

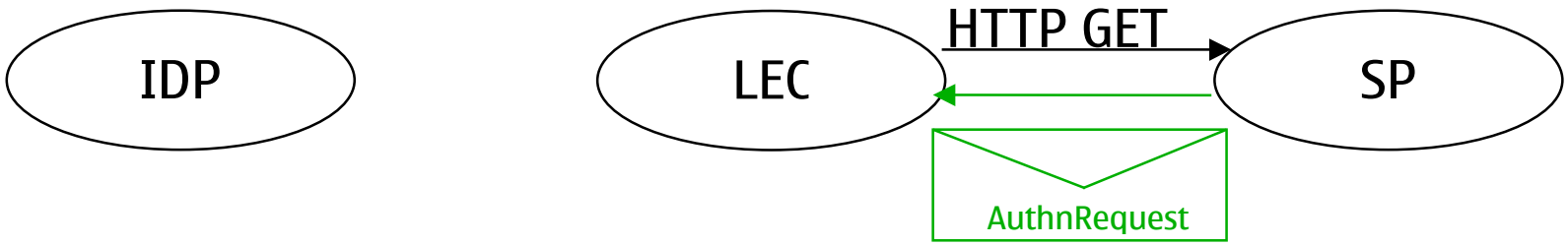
NOKIA

1. HTTP Request



- HTTP Headers indicate support for LECP

2. Authentication request



AuthnRequestEnvelope

- AuthnRequest – the Liberty 1.1 authentication request
- ProviderId – Identifier for SP
- ProviderName – Human readable name for SP
- IDPList – list of IDPs acceptable to SP, optional information for LEC
- IsPassive – if “true”, do not interact with principal

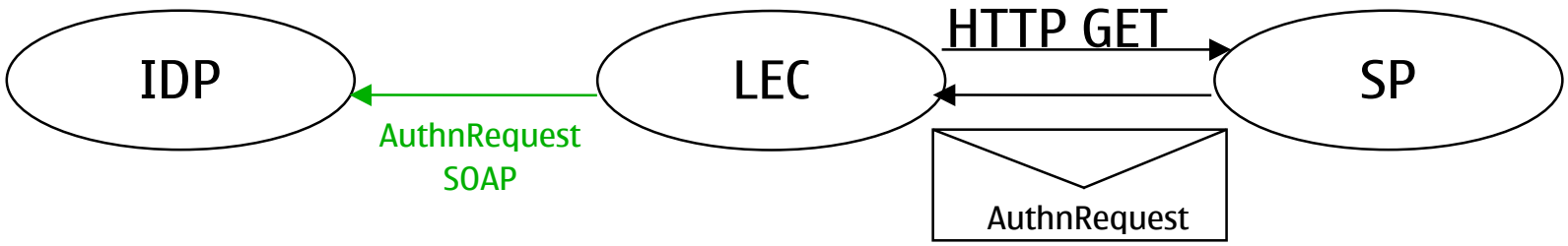
AuthnRequest

- Extends SAML 1.0 samlp:RequestAbstractType type
- Extended with elements:
  - ProviderID – URI identifier for SP
  - ForceAuthn – if “true”, reauthenticate
  - IsPassive – if “true” IDP must not interact with principal
  - Federate – if “true”, SP wishes to federate with IDP
  - ProtocolProfile – which profile to use for response
  - AuthnContext – authentication context desired by SP
  - RelayState – information to relay back in response
  - AuthnContextComparision – exact, minimum, better
- Attribute “id”

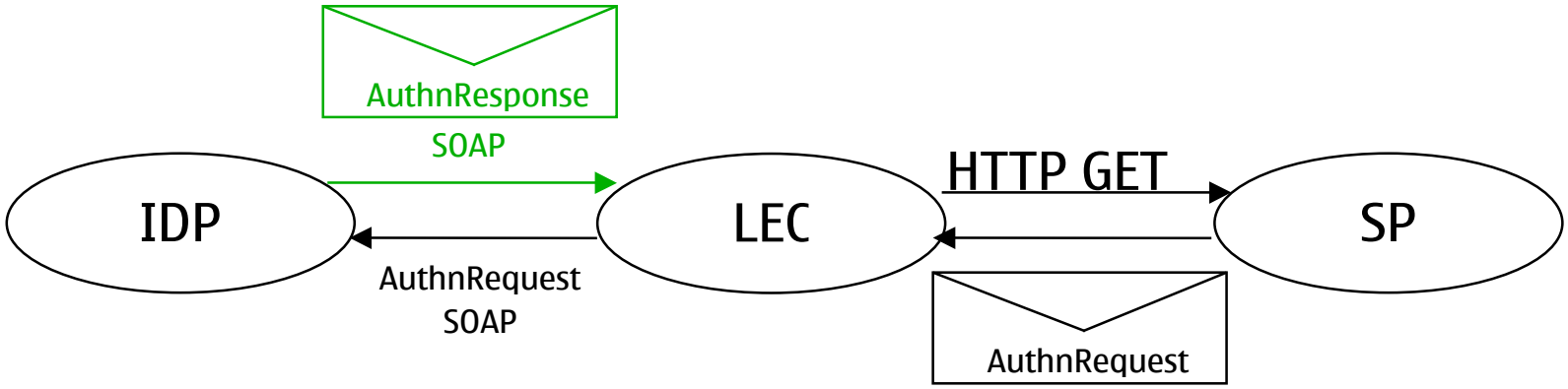
3. LEC Processes authentication request

- Determine proper IDP
  - SP, principal
  - Possible principal interaction
  - Optional SP IDPList
- Send authentication request to IDP

4. IDP Authentication Request



5. IDP Authentication Response



AuthnResponseEnvelope

- AuthnResponseEnvelope
  - AuthnResponse
  - AssertionConsumerServiceURL – URL IDP anticipates based on MetaData

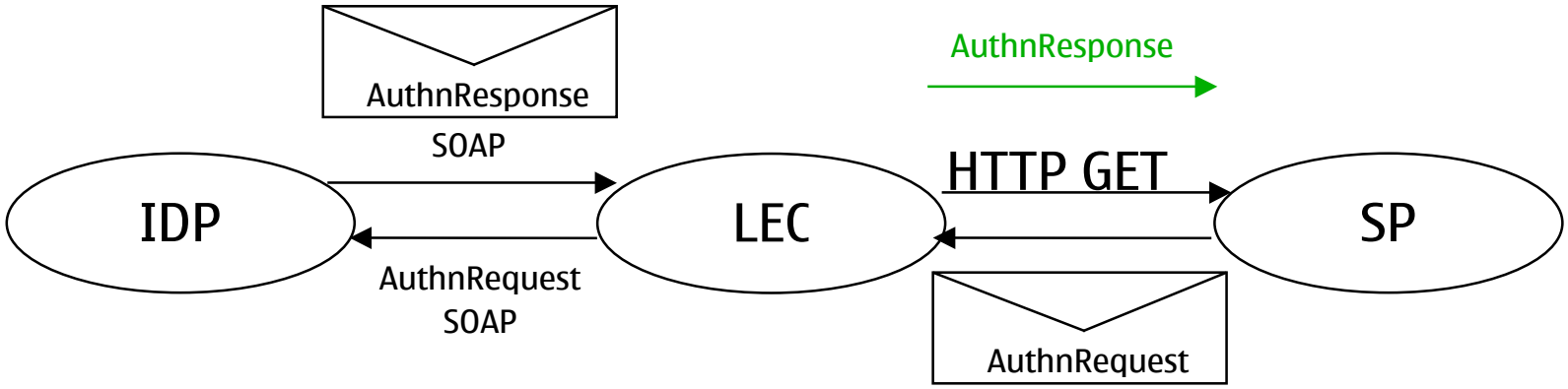
AuthnResponse

- Extends SAML 1.0 samlp:ResponseType type
- Extended with elements:
  - ProviderID – URI identifier for SP
  - RelayState – information to relay back in response
- Attribute “id”

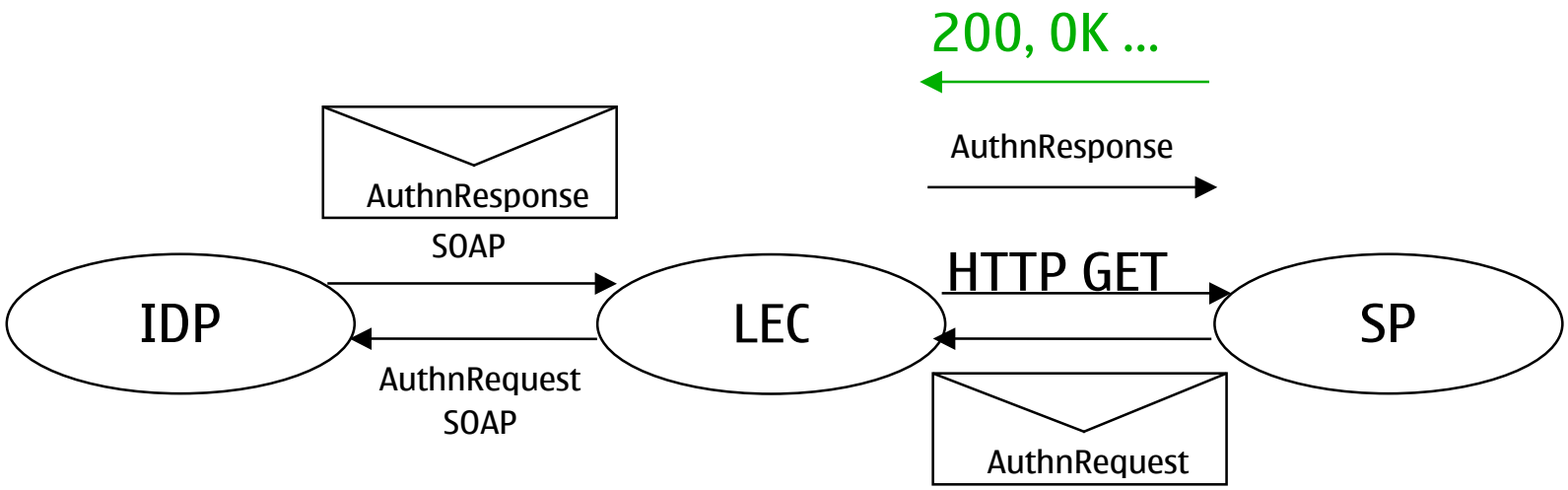
6. LEC Processes response

- Validate return destination
  - Anticipated response destination vs IDP expected destination

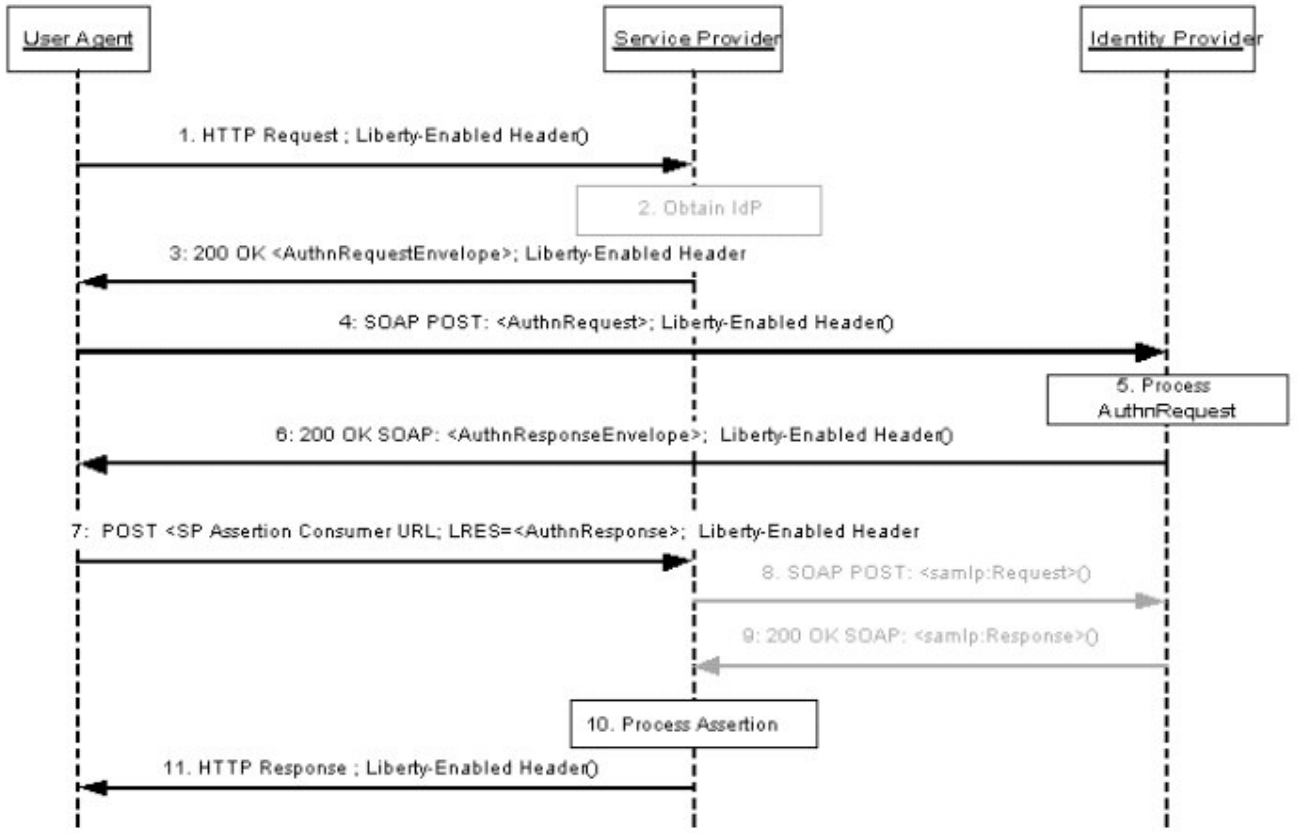
7. Authentication response to SP



8. SP Response to original request



LECP: Profile



NOKIA