Naming Objects in DECADE In-Network Storage

Dirk.Kutscher@neclab.eu

IETF-82, Taipei

IRTF ICN Side Meeting

Accessing Named Information

- Want to have some assurance on name-data integrity
  - Did I get what I asked for?
  - Provenance?

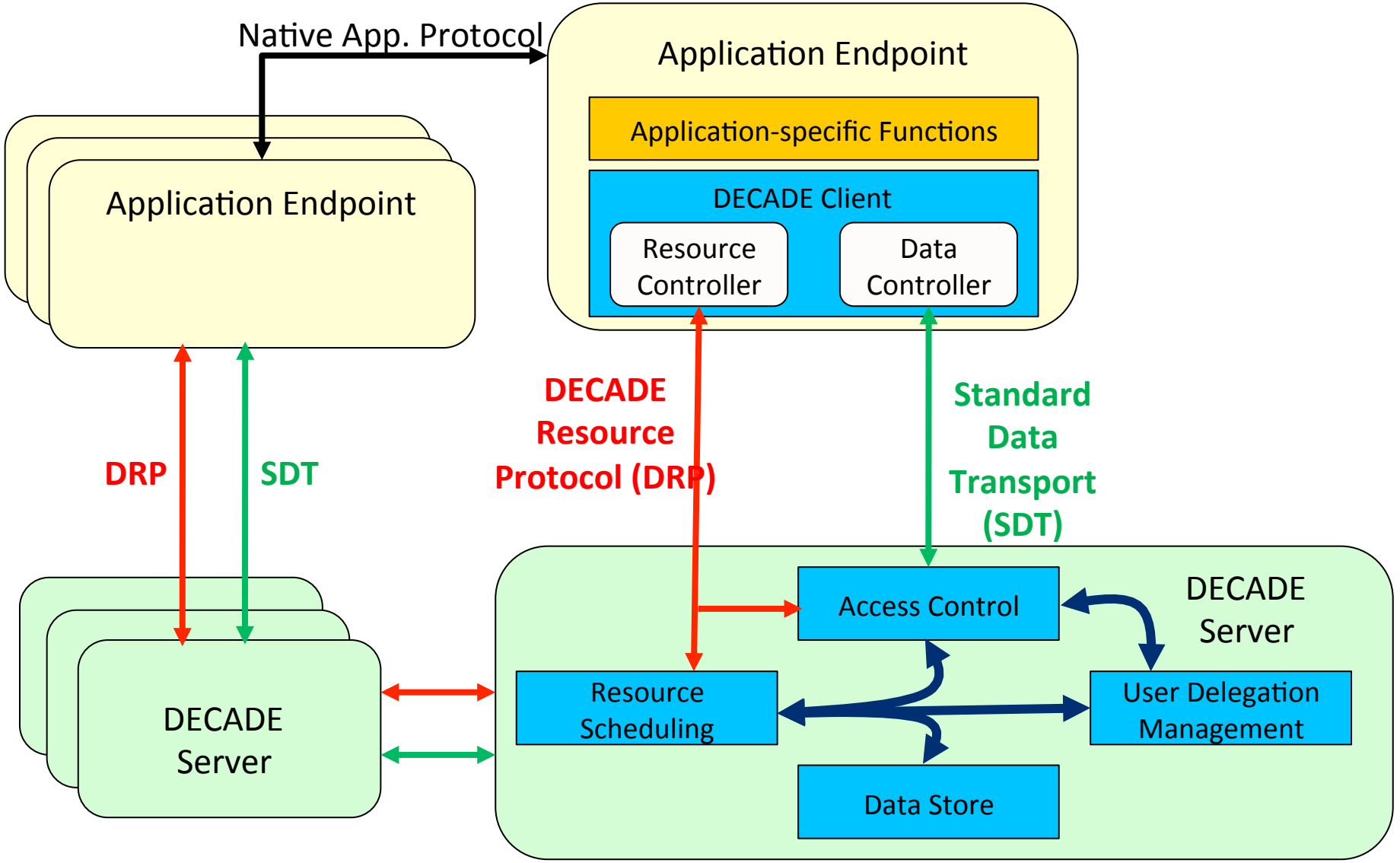
- Different applications, architectures have different requirements
  - Content hashes
  - Owner PK hashes (in conjunction with other security data in body)
  - New ideas

Note

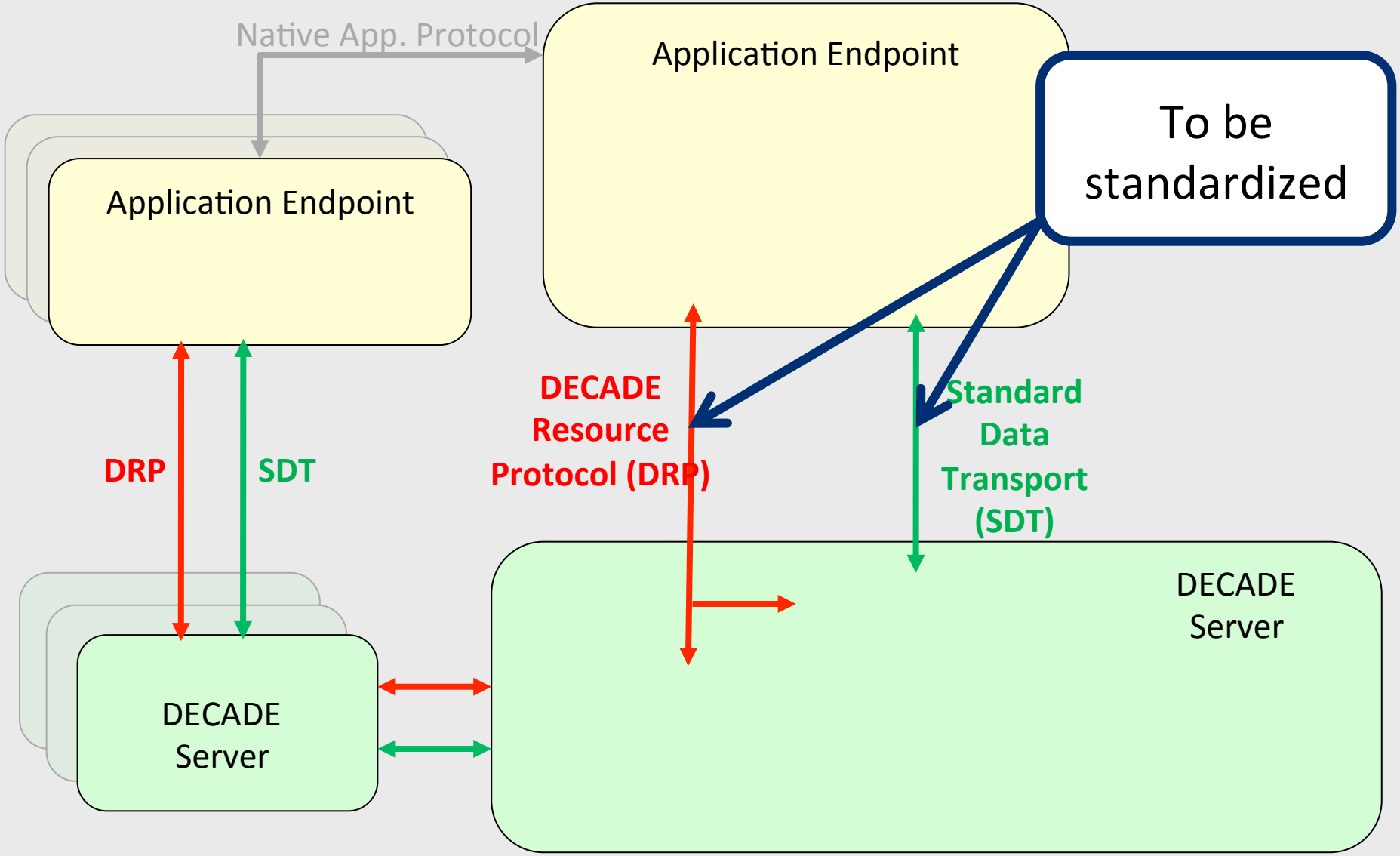
- Work done by Stephen Farrell, Phillip Hallam-Baker, Börje Ohlman, Christian Dannewitz, Rob Stradling, Dirk Kutscher

- In progress – a proposal at this time

Decoupled Control and Data Planes



Decoupled Control and Data Planes



Naming

- DECADE architecture requirements:
  - Globally unique names
  - Application-independent
  - Name-content binding through hashes

- URIs for Named Information
  - http://tools.ietf.org/html/draft-farrell-decade-ni-00
  - http://tools.ietf.org/html/draft-hallambaker-decade-ni-params-00
  - Key function: representing object hashes, with hash identifier
  - Support for different hash algorithms
  - Extensibility mechanism for application-specific URI parameters
  - Defined mapping from NI URIs to HTTP URIs

```
ni:///sha-256;B_K97zTtFuOhug27fke4_Zgc4Myz4b_lZNgsQjy6fkc
```

```
ni://example.com/sha-256;B_K97zTtFuOhug27fke4_Zgc4Myz4b_lZNgsQjy6fkc?ct=image/jpeg
```

Extension Mechanism

```
ni://example.com/sha-256;B_K97zTtFuOhug27fke4_Zgc4Myz4b_lZNgsQjy6fkc?ct=image/jpeg
```

- Extensions via URI query parameters
  - Not relevant for determining identity
- "params" draft defines optional, "advanced" stuff
  - Truncated hashes
  - Dynamic content handling
  - Content type
  - Additional locators
  - Decryption key

How to use NI Names in DECADE

- Equality testing works on algoritm identifier and actual hash value
  - All other elements (including authority) are not considered
  - **DECADE should not require an authority field**

```
ni://example.com/sha-256;B_K97zTtFuOhug27fke4_Zgc4Myz4b_lZNgsQjy6fkc
```

```
http://example.com/.well-known/ni/sha-256/B_K97zTtFuOhug27fke4_Zgc4Myz4b_lZNgsQjy6fkc
```

- Mapping to HTTP
  - NI defines one specific mapping
  - Clearly only useful for HTTP-based DECADE
  - May impose some constraints on server configurations

Other NI Functions for DECADE

- Locator specification
  - Useful for referring client to a specific DECADE server
  - Implementable using an extension parameter

```
ni:///sha-256;B_K97zTtFuOhug27fke4_Zgc4Myz4b_lZNgsQjy6fkc
     ?decade-loc=http://example.com/decade/NAME
```

DECADE NI profile

- Content type: already in NI params spec

- Authentication token

```
ni:///sha-256;B_K97zTtFuOhug27fke4_Zgc4Myz4b_lZNgsQjy6fkc
     ?decade-auth=dhek4nd2kj2j
```

Other Envisaged Usages (beyond DECADE)

- WEBSEC
  - NI drafts presented to DECADE and WEBSEC
- Content identifiers in connectivity-challenged ICNs
  - http://tools.ietf.org/html/draft-farrell-dtnrg-bpq-00
- Other forms of name-data integrity
  - DONA P:L names (hash of publisher's PK + label)
  - => new algorithm specifier for NI URIs

More Discussion

- DECADE Meeting
  - Thursday, 1740-1940 Afternoon Session III
  - Room 101C