Group Key Encryption

Christopher A. Wood
UCI and PARC

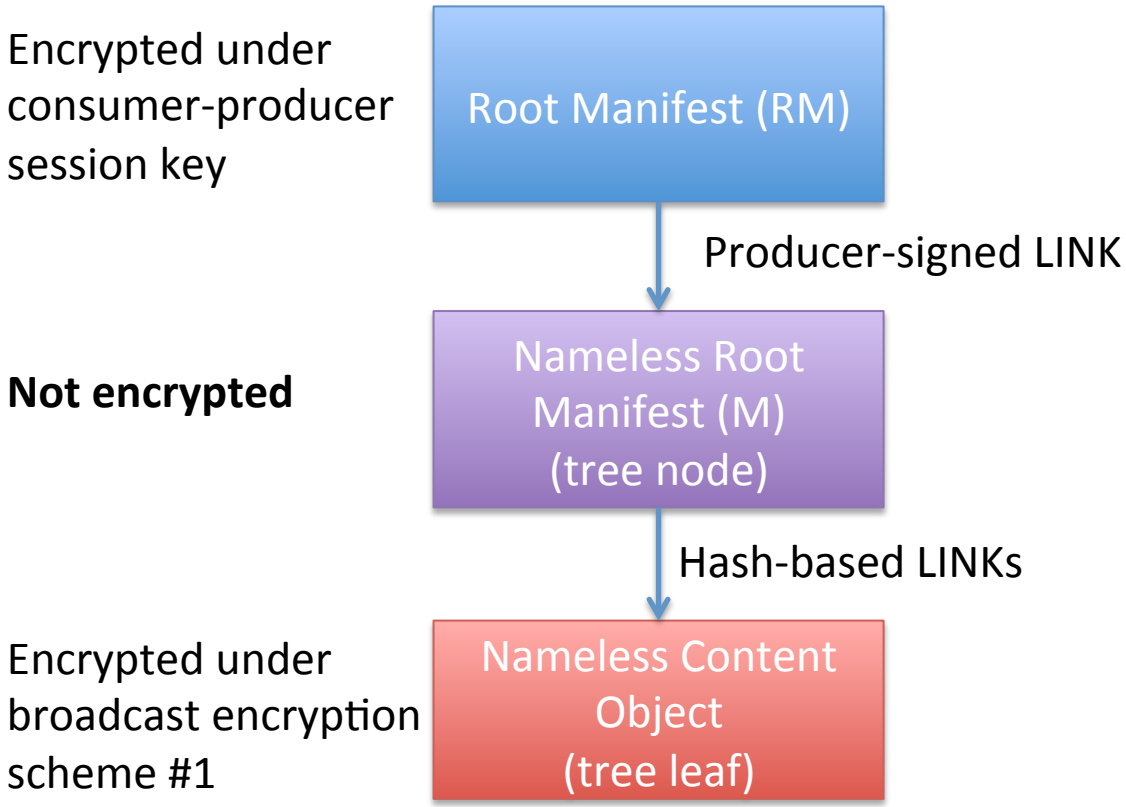
ICNRG Interim Meeting – IETF 96 – Berlin

July 17, 2016

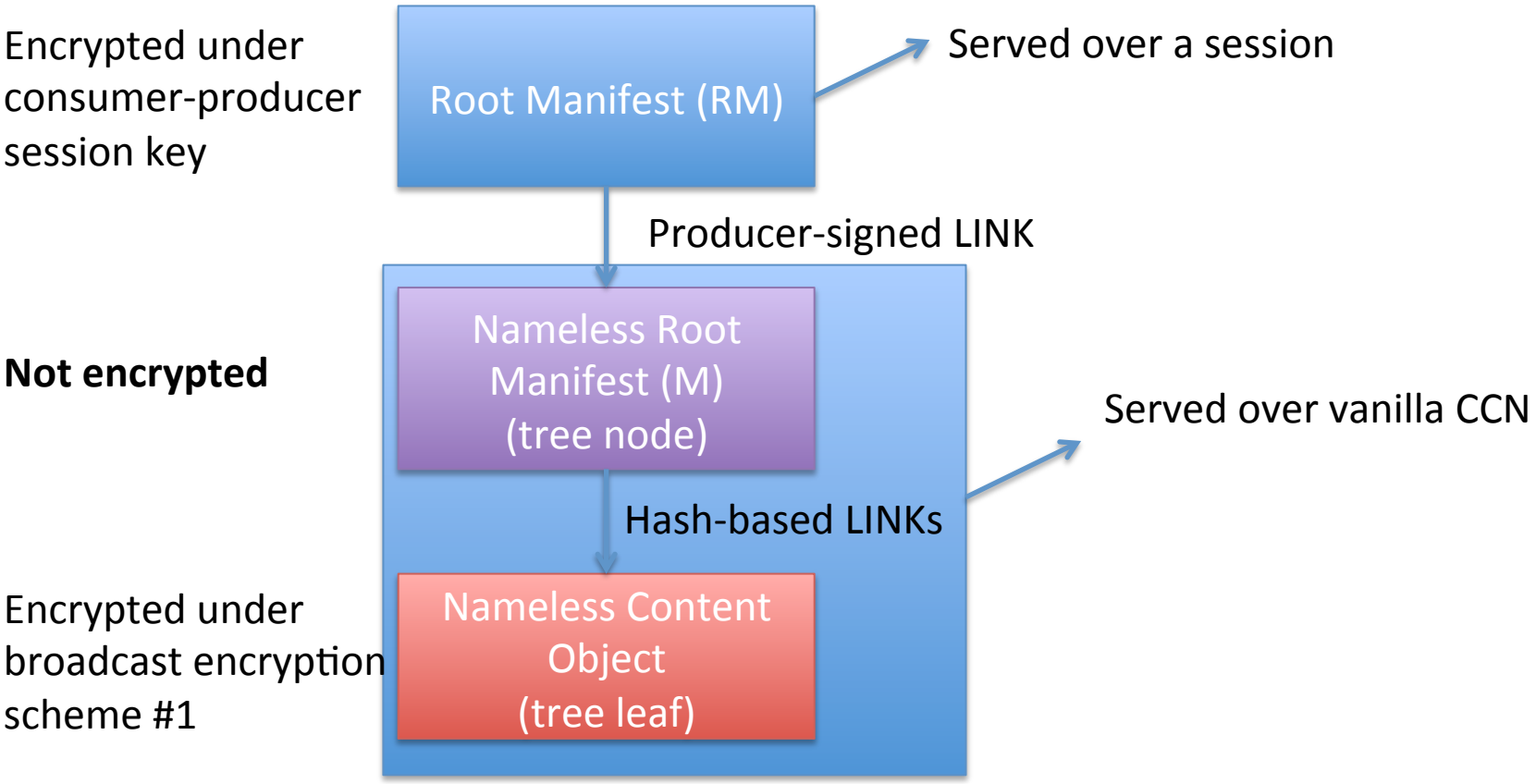
Goal

- Specify how to encrypt **single pieces of data** under a common group key
  - *Not how to manage that group key*
- Defer access control management of group keys to named data to a higher layer in the stack

Encryption Layers



Encryption Layers



Message Types

Root Manifest (RM)

Application-specific manifest (as a Content Object) that contains:

- Producer-signed LINK to M
- List of replica pointers (locators or LINKs)
- Encrypted content symmetric key

Nameless Root Manifest (M) (tree node)

Nameless CCNx FLIC Manifest

Nameless Content Object (tree leaf)

Nameless CCNx Content Object

Nameless Content Object Construction

- Input:
  - Symmetric data encryption key DEK
  - Content object C
- Output:
  - C with payload encrypted under DEK with AES-GCM

Nameless Manifest Construction

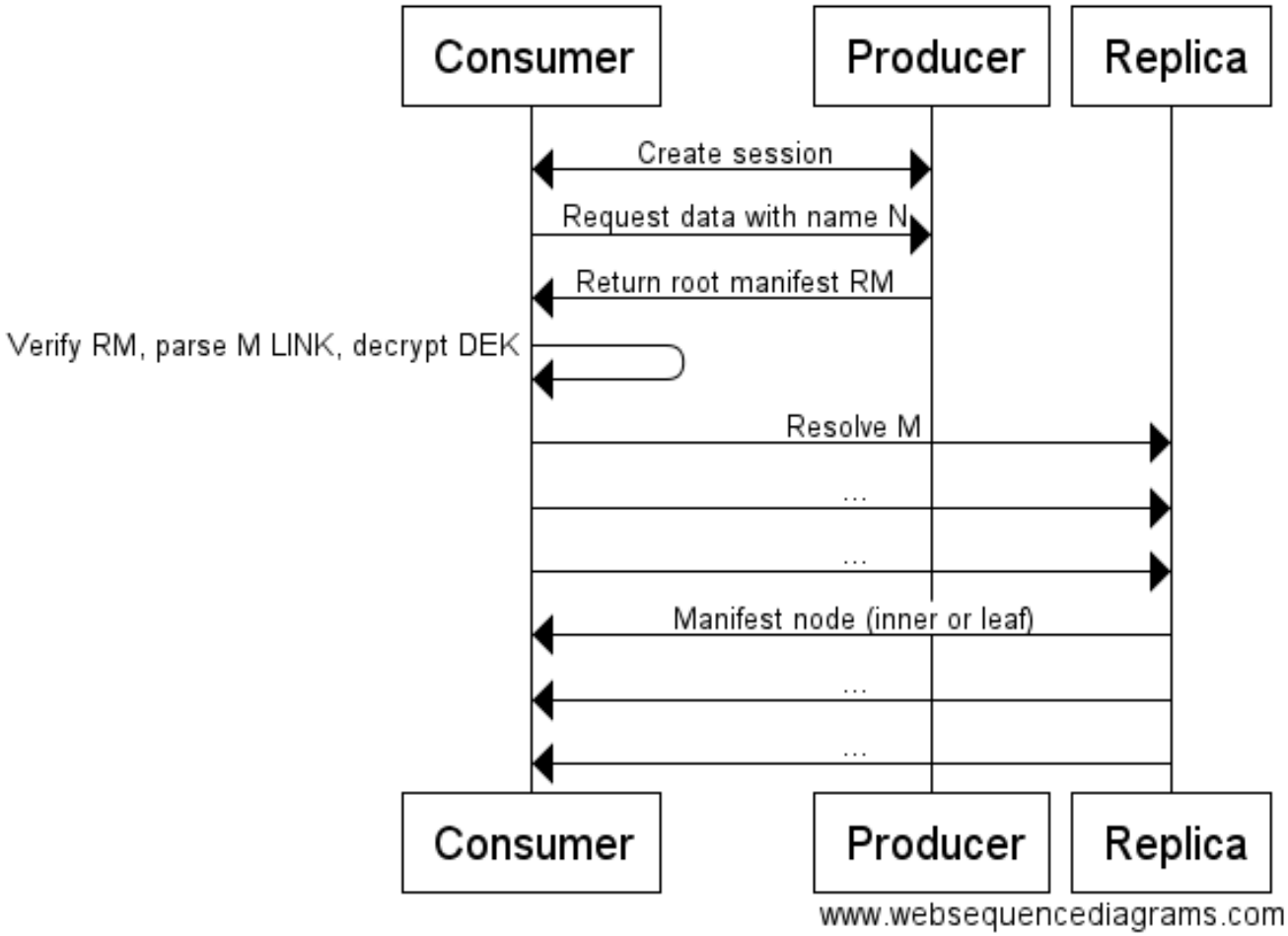
- Input:
  - Encrypted Content Object leaves C1,…,Cn
  - Symmetric data encryption key DEK
  - Recipient public broadcast key PK
  - Producer private key SK
  - Manifest name N
- Output:
  - DEK wrapped (encrypted) with PK
  - Nameless manifest tree T with root M built on the leaves
  - Signed link that binds H(M) to N

Root Manifest Construction

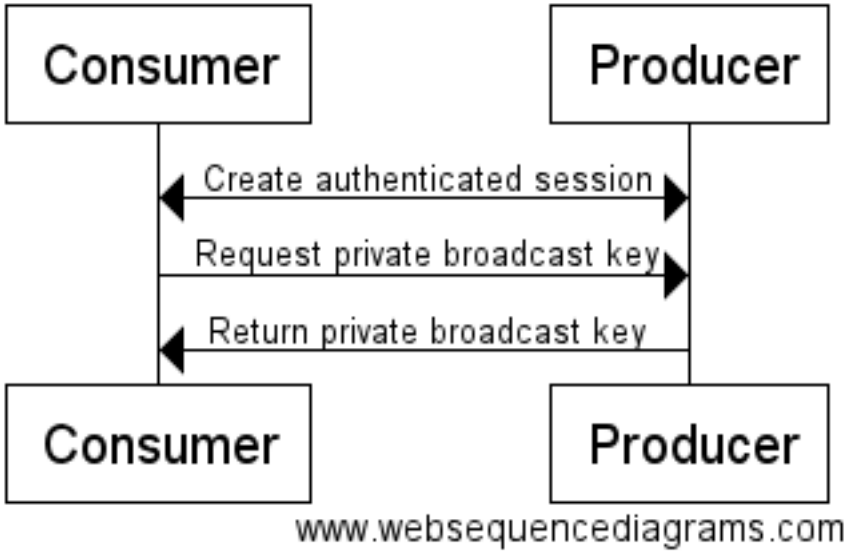
- Input:
  - Encrypted DEK under PK
  - Producer-generated link for T
  - Data name N
- Output:
  - **Content object** with name N a body containing the signed link and DEK

Note: we'll have to specify what the body of this "content object manifest" contains… but at a minimum it should carry the link and encrypted DEK

Protocol


Consumer
Producer
Replica
Create session
Request data with name N
Return root manifest RM
Verify RM, parse M LINK, decrypt DEK
Resolve M
...
...
Manifest node (inner or leaf)
...
...
Consumer
Producer
Replica
www.websequencediagrams.com

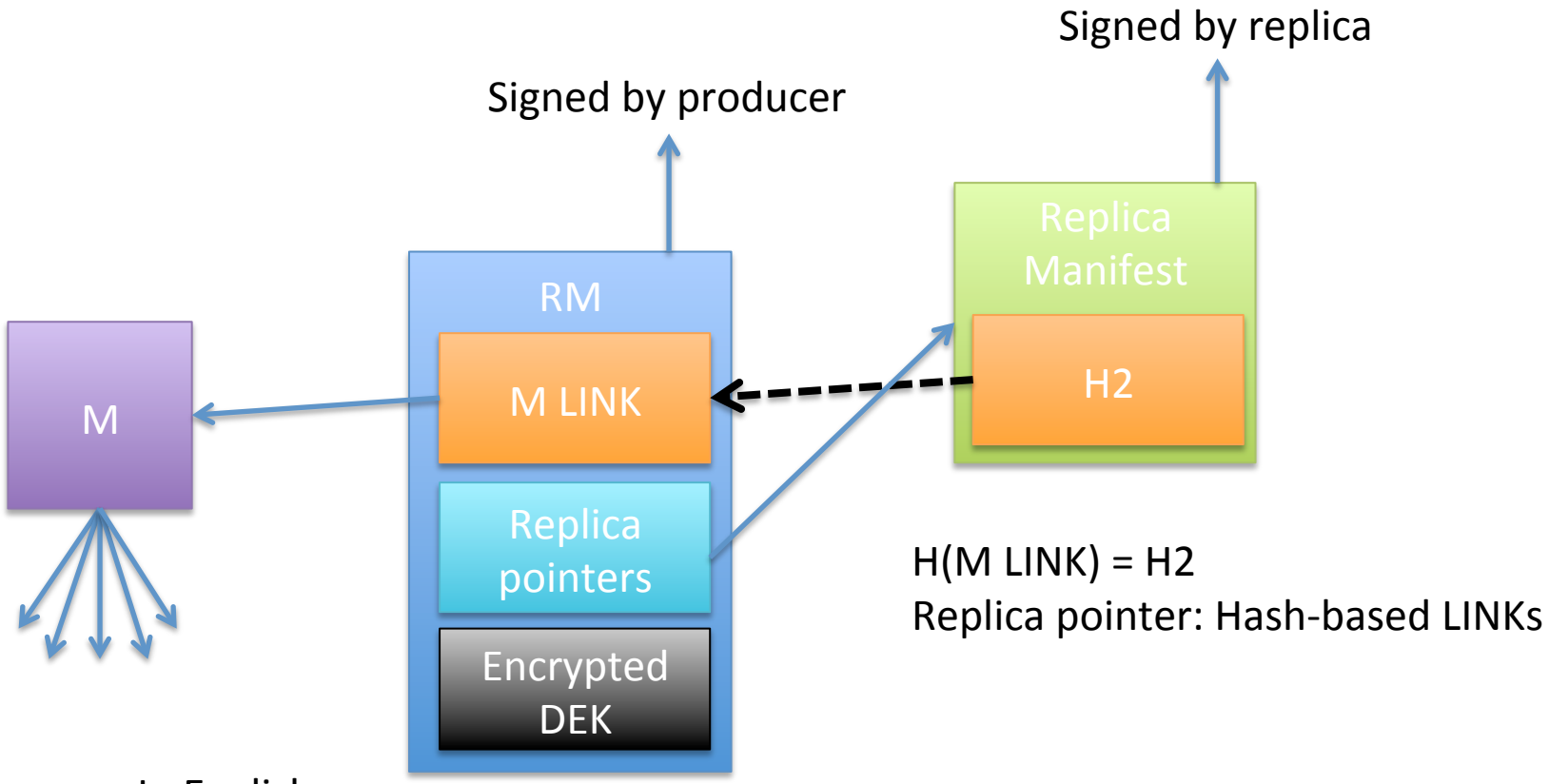
Obtaining Private Decryption Key



Lame Delegation

- Lame delegation is when RM points a namespace where M is not stored
- This occurs when the replica does not confirm the pointers in RM

Preventing Lame Delegation



In English:

- RM says M can be obtained at the replica
- The Replica Manifest says that M can be obtained under its namespace

Replica Manifest Construction

- Input:
  - M LINK
  - Replica names
  - Replica private key SK
- Output:
  - Replica manifest (signed by SK) with the hash of M LINK and list of replica names

Protocol with Lame Delegation