

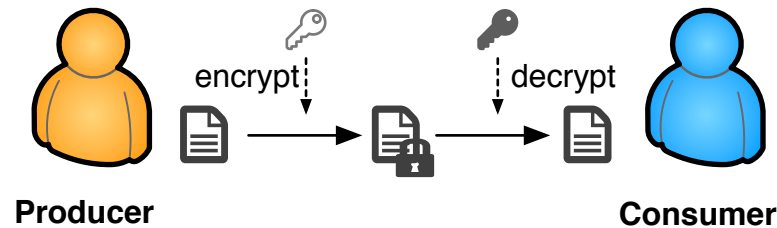
Controlled Sharing of Sensitive Content

NDN Case Study

Yingdi Yu
UCLA

Content-based confidentiality

- Confidentiality stays with content
 - independent from where the content is
 - independent from how it is delivered
 - content are produced in encrypted format
 - only authorized consumers are able to access the content



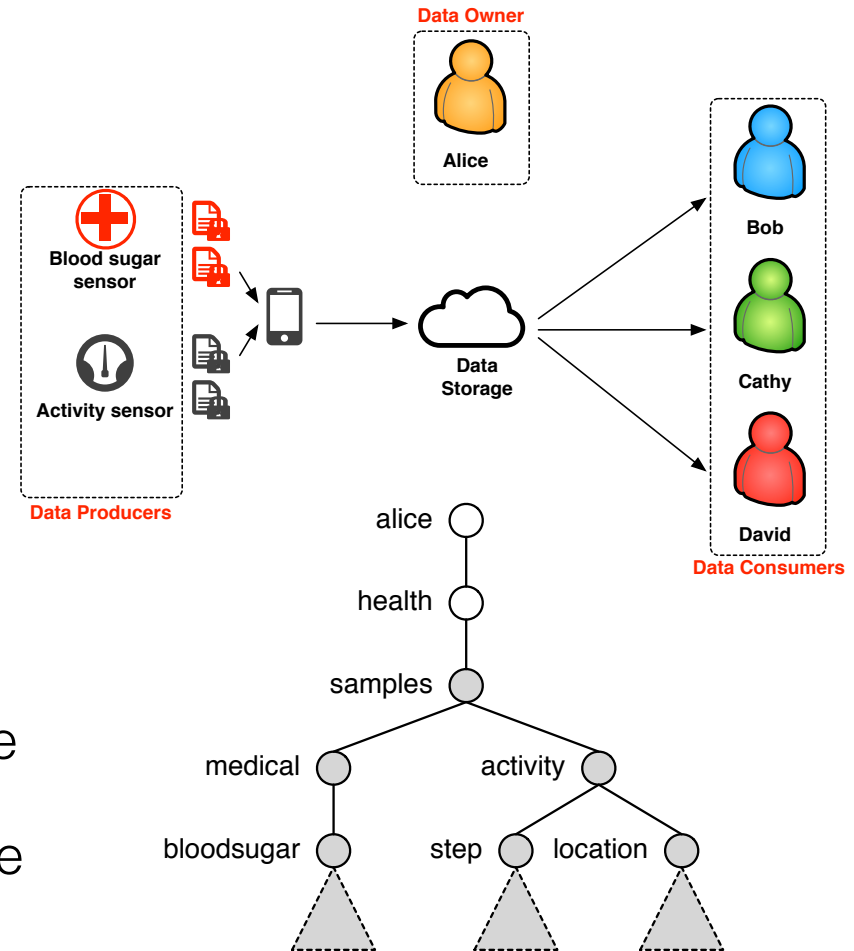
- Application-level end-to-end confidentiality
 - not just the end of a connection
 - multi-party communication

Req. on confidentiality

- Encryption requires careful design
 - differential confidentiality
 - different content may be visible to different groups of consumers
 - flexibility
 - retain the ability of changing access
 - scalability
 - keep reasonable number of encryption keys
 - avoid unnecessary re-encryption/signing
 - forward secrecy
 - make encryption keys less dependent on other keys
- Content encryption should not block data production

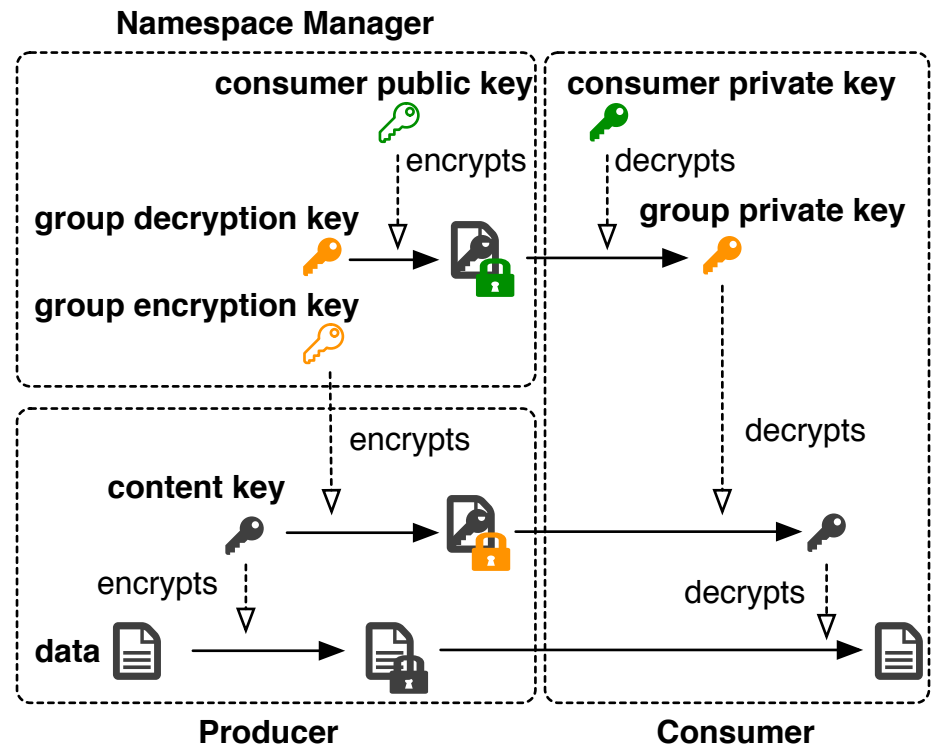
Application driven approach

- NdnFit
 - distributed production
 - a group of producers under the same name space
 - differential confidentiality
 - different consumers may access different content
 - online data sharing
 - producer can freely produce encrypted content without knowing who can access the content



Encryption Scheme

- Separate content production from access control
 - producer-created content key
- Control access through a group key
 - created by namespace manager
 - distributed by namespace manager
 - public key in current implementation
- Producers retrieve group encryption key (public key), encrypt content key properly
- Consumers retrieve group decryption key (encrypted private key)

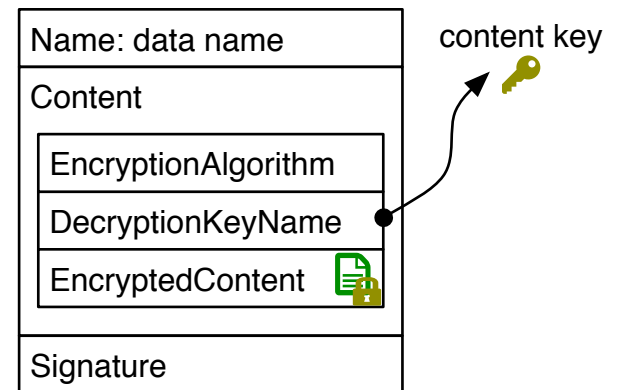


Name-based Access Control

- Name of group encryption key serves as access control instruction
 - `/<data_prefix>/E-KEY/<additional_restriction>`
 - `/alice/health/read/activity/E-KEY/20150930160000/20150930180000`
 - scope: any Alice's activity data produced during Sep 30, 4pm-6pm
- Producer retrieves group encryption key, encrypts content keys falling into the scope
 - `/alice/health/samples/activity/steps/C-KEY/20150930170000/20150930180000`
 - encrypt Alice's step data produced during Sep 30, 5pm-6pm

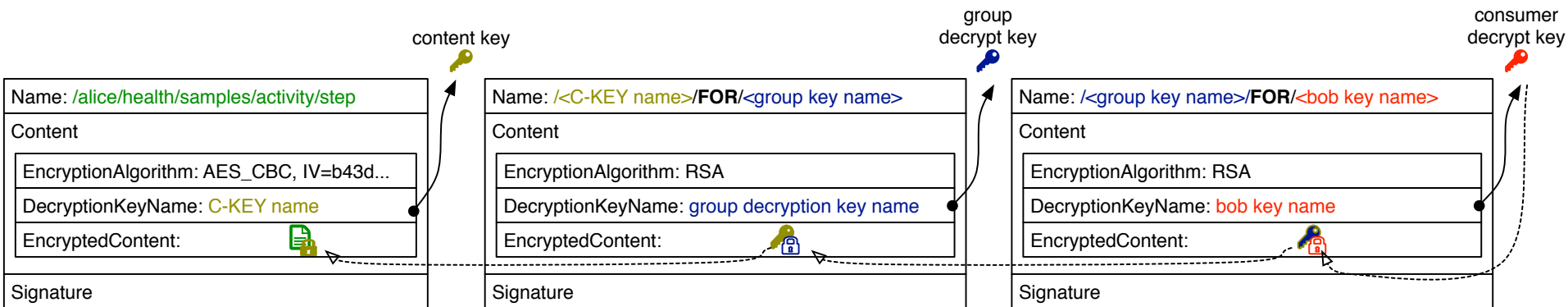
Encrypted Content Format

- Data packet must carry enough information for authorized consumers to decrypt content
- Experiment as application semantics
 - content encoding
 - not a part of architecture yet
- Three sub-TLVs:
 - EncryptionAlgorithm
 - may also algorithm-specific fields,
 - e.g., Initial Vector
 - DecryptionKeyName
 - facilitate decryption key retrieval
 - EncryptedContent
- When a data has more than one encrypted copies
 - each encrypted copy is an independent data packet
 - naming convention: /<content_name>/FOR/<decrypt_key_name>



Content production/consuming

- Producer create a symmetric key (content key) to encrypt content
 - content key has the minimum granularity, e.g. one hour
 - `/alice/health/samples/activity/steps/C-KEY/20150928080000/20150928090000`
- Producer retrieves group encryption key from namespace manager
 - encrypt content key using a group encryption key if the content key name falls into the scope of the group encryption key
 - `/alice/health/samples/activity/steps/C-KEY/20150928080000/20150928090000/FOR/alice/health/read/activity`
- Consumer decrypts content by constructing a decryption key chain
 - retrieve encrypted content, encrypted content key, encrypted group decryption key



- Application library will be available in next NDN platform release

Open questions

- Enable forward secrecy: decouple consumer private key with content key
 - key distribution services
- Name privacy
- Convert key exchange between namespace manager and producers to identity-based encryption, attribute-based encryption
- Access revocation
- Secure multi-party computing

Summary

- Content-based confidentiality makes confidentiality of content location-independent
- Content should be carefully encrypted to achieve flexible and scalable access control at fine granularity
- Expressive NDN name can be leveraged for efficient access control
- More encryption schemes need to be explored to address remaining issues