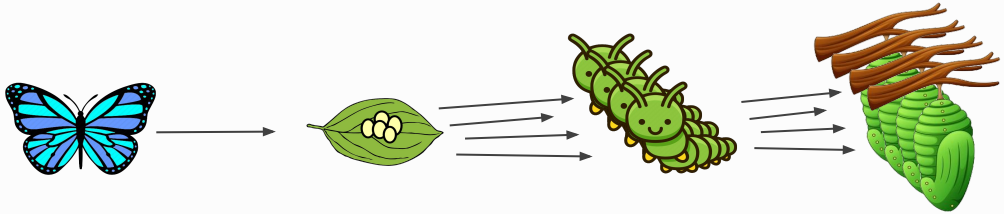


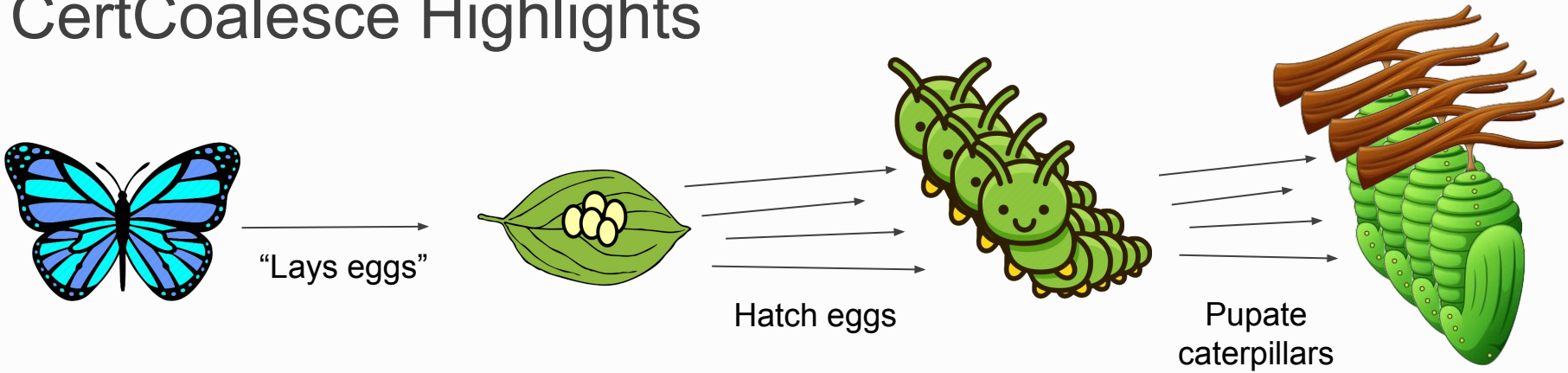
CertCoalesce

Butterfly Key Expansion to Manage NDN Certificate Pools

Proyash Podder, Xinyu Ma, Alex Afanasyev

11th NDN Hackathon Hack Presentation
May 23, 2021

CertCoalesce Highlights



(1)

Generate Butterfly key

(private + public key)

Define / agree on set size and definition

Certificate issuer operations

(2)

Expand Butterfly public key into a set for signing

(public key set)

(3)

Specialize and sign public keys in the set

(cert set)

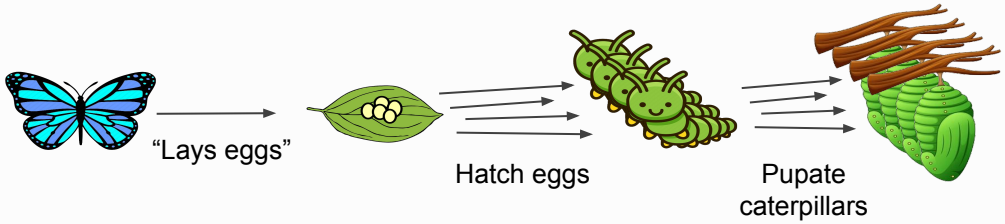
Device operations

(4)

Specialize and expand private keys

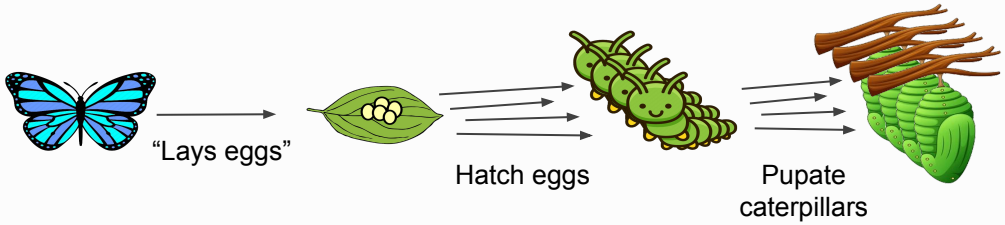
(private key set)

Design Properties



1. One butterfly key pair can generate specified (technically large number) cocoon certs that can be valid simultaneously
2. Set of private keys (and assumed set of certificates) can be used **after** confirmation (need a "kaleidoscope ID" to "pupate" caterpillars) of the signed set from the issuer
    a. In the future, this design feature may be adjusted
3. Set size (and actual timing for cert generation) is agreed upon between requester and issuer
    a. Right now, it is explicitly requested by the requester and set of certs is immediately generated by the issuer
    b. In the future, we could use a convention with scheduled cert generation by the issuer
4. Hatching (of a public key) and pupation (of a private) based on 64-bit identifier
    a. Identifier can be mapped to a time period
    b. Or hashed from a name (e.g., to request certs for nodes in hierarchy)

Design Details



Device

1. Generate private Butterfly
2. Derive public Butterfly
7. Derive Cocoon private keys
6. Decrypt Kaleidoscope

{i1,...,in}

Cocoon private key 1

Cocoon private key n

Cert Issuer

3. Generate Kaleidoscope
4. Encrypt Kaleidoscope
5. Derive Cocoon certificates

{i1,...,in}

Cocoon certificate 1

Cocoon certificate n

Send

Public butterfly

i set

kaleidoscope

Matching to NDN Key/Certificates

- Butterfly (private/public) key (“seed”) is more than just a regular key
  - ECC signing key + ECC encryption key + AES expansion function
  - **<identity>/KEY/butterfly-<key-id>**
    - **/coalesce/KEY/demo-1**
- Egg (public) keys are regular ECC public keys
  - Don’t really need to be stored independently, but have their names expanded from butterfly key + ID inside the pool
  - **<identity>/KEY/<key-id>-<ID-in-the-Pool>**
    - **/coalesce/KEY/demo-1-1, ..., /coalesce/KEY/demo-1-5**
- Caterpillar certs are regular NDN certificate
  - Payload: regular ECC public key + any relevant signing info (validity period, info, etc.)
  - **<identity>/KEY/<key-id>-<ID-in-the-Pool>/Coalesce/_version=<XX>**
    - **/coalesce/KEY/demo-1-1/coalesce/v=..., …, /coalesce/KEY/demo-1-5/coalesce/v=...**
- Cocoon private keys are also regular ECC private key
  - Can be directly stored and used in NDN Keychain
  - **<identity>/KEY/<key-id>-<ID-in-the-Pool>** (same as egg key names)
    - **/coalesce/KEY/demo-1-1, ..., /coalesce/KEY/demo-1-5**

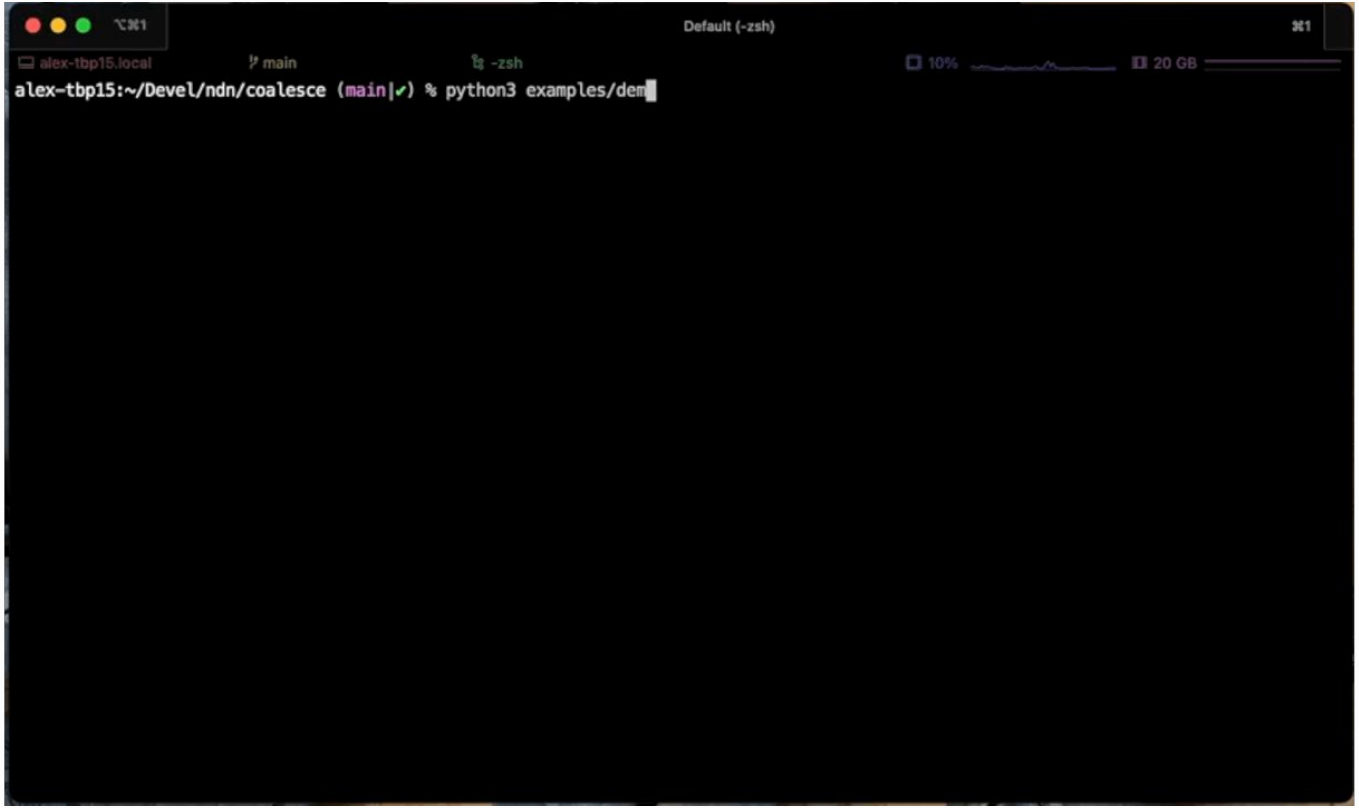
Hackathon Accomplishments

- (beyond original plan ✅) CertCoalesce design refinements
  - Initial sketch revealed issues, as a result design got changed (simplified)
  - Also, we renamed elements to closely match butterfly lifecycle
- (planned ✅) A working prototype of CertCoalesce crypto operations
  - Generating butterfly keys, laying and hatching eggs, pupating caterpillars
  - Generation of actual NDN certificates and private keys (ECC) to be directly used for signing and verification
- (planned ✅) Basic demo for CertCoalesce operations
  - Stay tuned, coming next
- (planned 🟨) Documentation
  - Refined algorithm description and created process diagram
  - But no interactive / expanded documentation
- (semi planned 🟨) Full integration with NDN
  - So far, only in-memory store of butterfly key (undefined encoding formats)

Future Work

- Determine format and implement encoding/decoding for butterfly key (public+private) storage
- Explore conventions for CertCoalesce pool identifiers
  - Time period and namespace based
- Explore key name expansion functions
- Evaluate uses of kaleidoscope ID
  - Generated by the issuer (now), supplied by the requester, hybrid
- Integrate with NDNCERT
- Expand documentation
  - Make it more comprehensive and interactive (if possible)

DEMO


Default (-zsh)
alex-tbp15.local
main
-zsh
10%
20 GB
alex-tbp15:~/Devel/ndn/coalesce (main|✔) % python3 examples/dem