

<http://ndncert.named-data.net>

NDNCERT: User Public Key Certification System for NDN Testbed

Alex Afanasyev (UCLA)

September 4, 2014

Goals

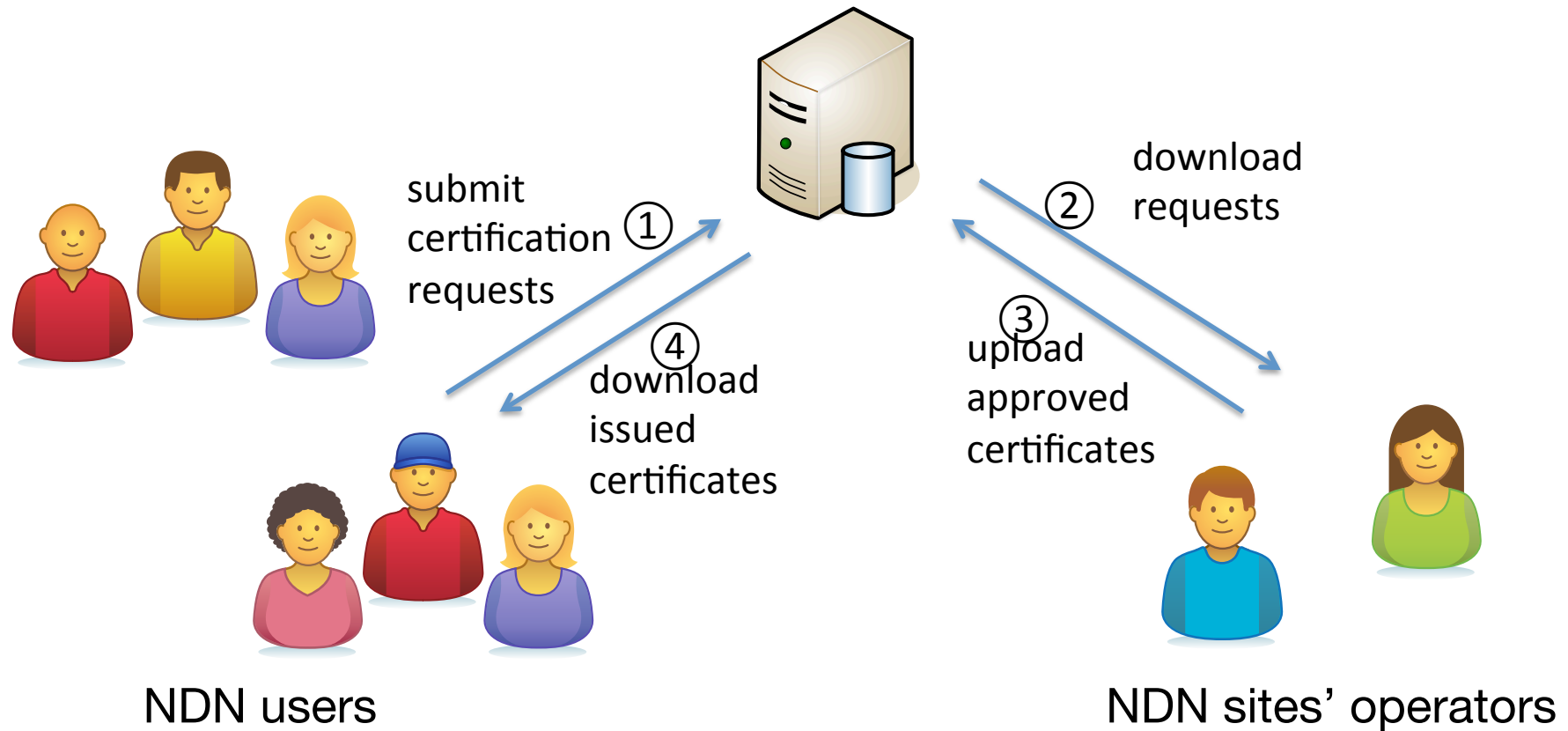
- Simplify and automate public key certificate process, yet keep it secure
 - simple for NDN testbed users to submit application for certificate and retrieve certificate (if approved)
 - simple for NDN testbed site operators to approve, issue and publish certificates
- Keep operators in the loop
 - The system automatically validates only email
 - Operators need to validate name, affiliation, etc.

Name conventions for NDN certificates

- Certificate namespace based on institutional email address*
 - tom@cs.ucla.edu -> /ndn/edu/ucla/cs/tom
- Request to approve certificate within institutional namespace are automatically directed to NDN site's operator
 - UCLA operator for tom@cs.ucla.edu (/ndn/edu/ucla/cs/tom)
 - WashU operator for bob@wustl.edu (/ndn/edu/wustl)
- * Non-institutional addresses and addresses of institutions that are not part of testbed assigned guest NDN namespace:
 - alex@gmail.com -> /ndn/guest/alex@gmail.com

Certification system overview

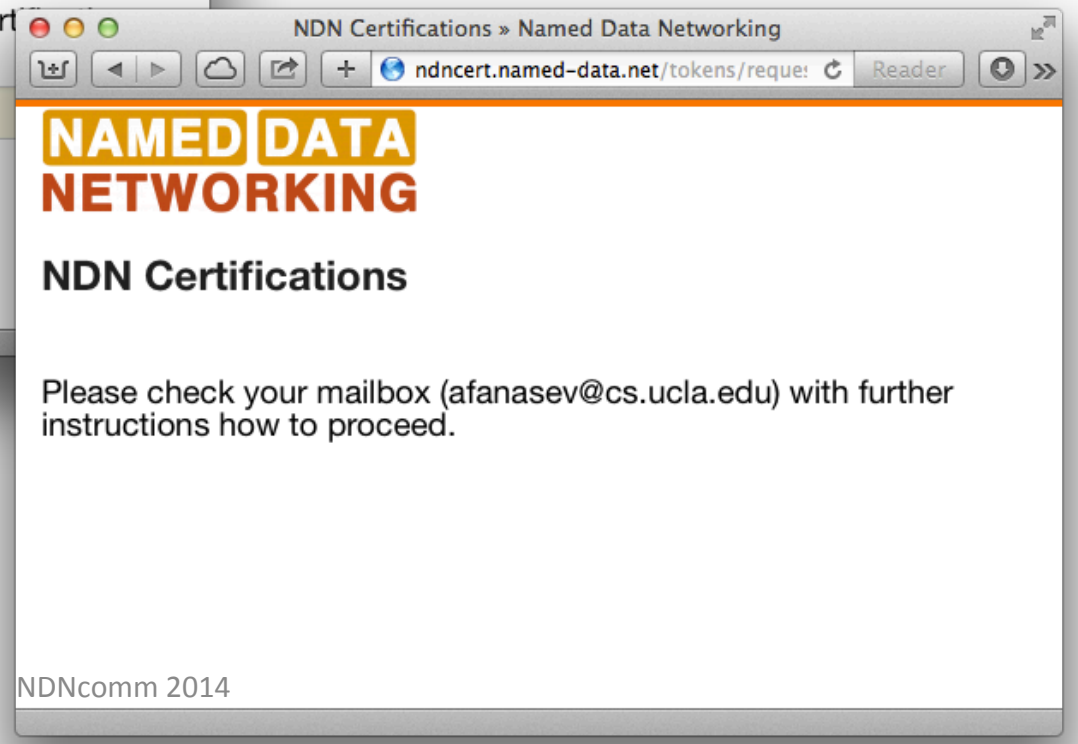
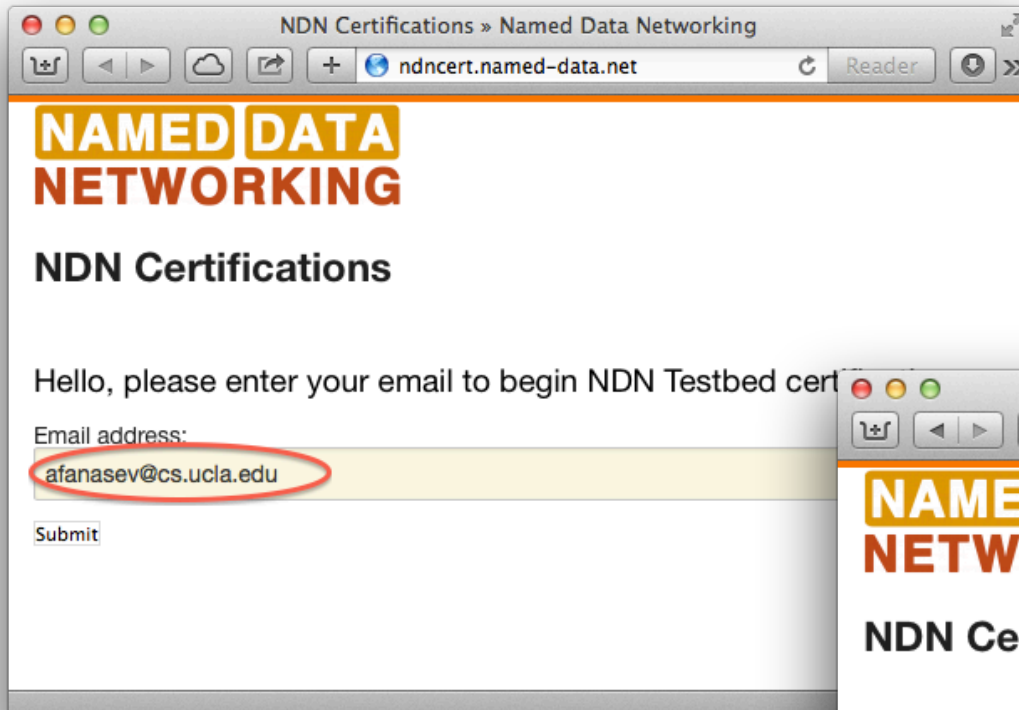
<http://ndncert.named-data.net>



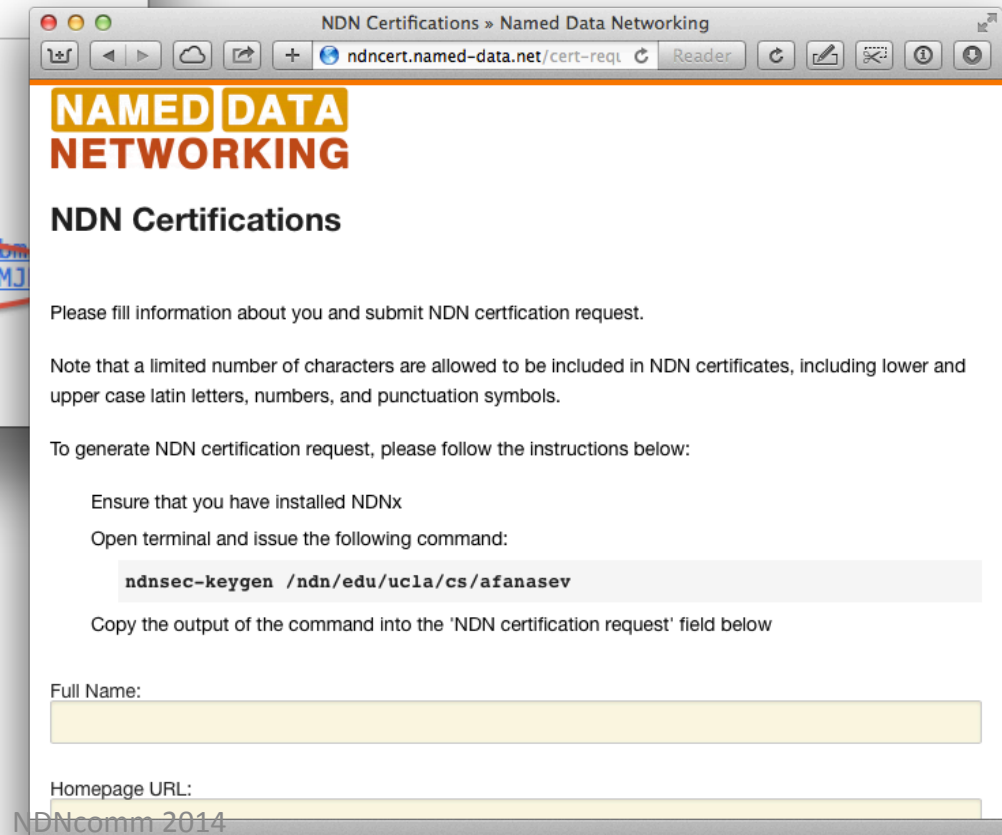
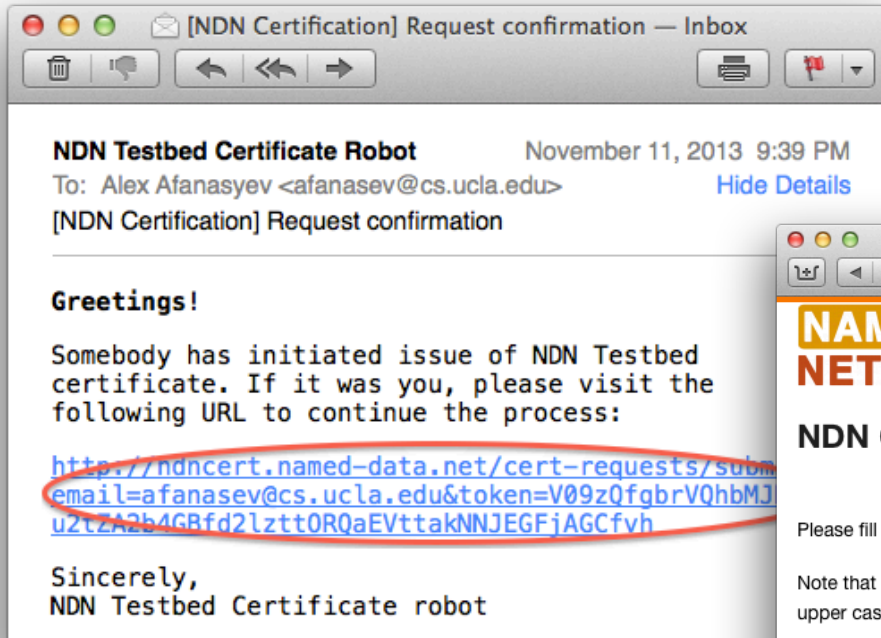
User guide

1. Go to <http://ndncert.named-data.net>, initiate certification by submitting email address
2. Check mailbox and click to open certification submission page
3. Generate certification request in the specified namespace (derived from email)
4. Submit name, other information to associate with the certificate, and public key
5. Wait for email notification of the approval by the site's operator
6. Follow the instructions to install the issued certificate

1. Go to <http://ndncert.named-data.net> and initiate certification by submitting email address



2. Check mailbox and click to open certification submission page



3. Generate certification request in the specified namespace (derived from email)

To generate NDN certification request, please follow the instructions below:

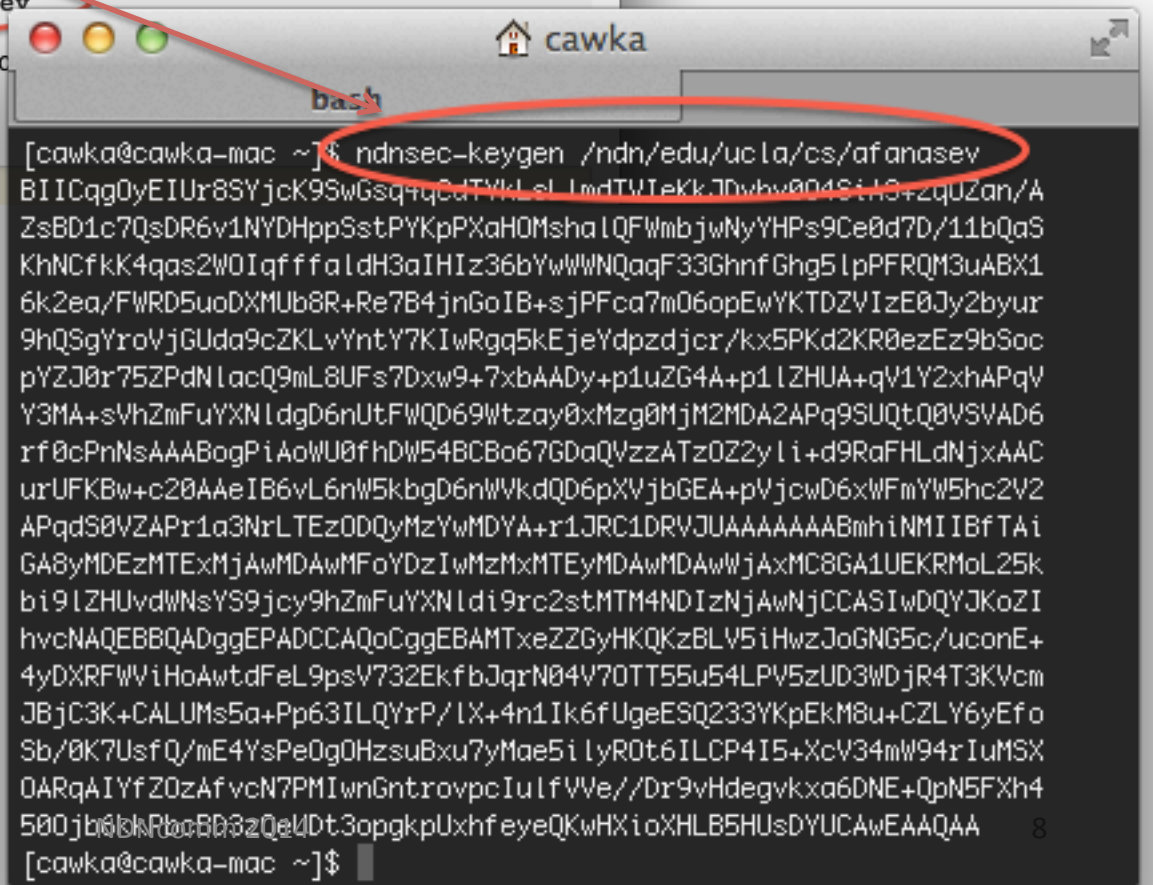
Ensure that you have installed NDNx

Open terminal and issue the following command:

```
ndnsec-keygen /ndn/edu/ucla/cs/afanasev
```

Copy the output of the command into the 'NDN certifi

Full Name:



```
[cawka@cawka-mac ~]$ ndnsec-keygen /ndn/edu/ucla/cs/afanasev
BIICqg0yEIUr8SYjck9SWSsq+qcdTYkLslLmdTWIekkJDyhw004S+iS+zqUZan/A
ZsBD1c7QsDR6v1NYDHppSstPYKpPXaHOMshaLQFWmbjwNyYHPs9Ce0d7D/11bQaS
KhNCfkk4qas2W0IqffaldH3aIHIZ36bYw/WNqaqF33GhnfGhg5lpPFRQM3uABX1
6k2ea/FWRD5uoDXMUb8R+Re7B4jnGoIB+sJPFca7m06opEwYKTDZVIzE0Jy2byur
9hQsGyroVjGUda9cZKLvYntY7KIwRgq5kEjeYdpzdjcr/kx5PKd2KR0ezEz9bSoc
pYZJ0r75ZPdNlacQ9mL8Ufs7Dxw9+7xbAADy+p1uZG4A+p1LZHUA+qV1Y2xhAPqV
Y3MA+sVhZmFuYXNldgD6nUtFWQD69Wtzay0xMzg0MjM2MDA2APq9SUQtQ0VSVAD6
rf0cPnNsAAABogPiAoWU0fhDW54BCBo67GDaQVzzATzOZ2yLi+d9RaFHLdNjxAAC
urUFKBw+c20AAeIB6vL6nW5kbgD6nWkDQD6pXVjbGEA+pVjcwD6xWFmY5hc2V2
APqdS0VZAPr1a3NrLTEz0DQyMzYwMDYA+r1JRC1DRVJUAAAAAABmhiNMIIBfTAi
GA8yMDEzMTEXMjAwMDAwMFoYDzIwMzMxMTEyMDAwMDAwWjAxMC8GA1UEKRMoL25k
bi9LZHUvdWNsYS9jcy9hZmFuYXNldi9rc2stMTM4NDIzNjAwNjCCASIdQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBAMTxeZZGyHKQKzBLV5iHwzJoGNG5c/uconE+
4yDXRFWwiHoAwtDFeL9psV732EkfbJqrN04V70TT55u54LPV5zUD3WDjR4T3Kvcm
JBjC3K+CALUMs5a+Pp63ILQYrP/LX+4n1Ik6fUgeESQ233YKpEKM8u+CZLY6yEfo
Sb/0K7UsfQ/mE4YsPe0g0HzsuBxu7yMae5ilyR0t6ILCP4I5+XcV34mW94rIuMSX
0ARqAIYfZ0ZafvcN7PMIwnGntrovpcIuLfvVe//Dr9vHdegvKxa6DNE+QpN5FXh4
500jbt6bNRbcBD3zQeUDt3opgkpluxhfeyeQKwHXioXHLB5HUsDYUCAwEAAQAA
[cawka@cawka-mac ~]$
```


4. Submit name, other information to associate with the certificate, and public key

```
cawka
bash
[cawka@cawka-mac ~]$ ndhsec-keygen /ndn/edu/ucla/cs/afanasev
BIICqgOyEIUr8SYjck9SswGsq4qCdTYkLsL lmdTVIeKkDdvby004S1A3+zaqUZan/A
ZsBD1c7QsDR6v1NYDHppSstPYKpXaHOMsha lQFwmbjwNyYHPs9Ce0d7D/11bQa5
KhNCFKK4qas2W0Iqf ffa l dH3aIHIz36bYwWNQagF33Ghnf Ghg5 l pPFRQM3uABX1
6k2ea/FWRD5uoDXMub8R+Re7B4jnGoIB+s jPFca7m06opEwYKTDZVIzE0Jy2byur
9hQsGyroVjGUda9cZKlvYntY7KIwRga5Ke jeYdpzdjcr /kx5PKd2KR0ezEz9bSoc
pYZJ0r75ZPdN l acQ9mL8UFs7Dxw9+7xbAADy+p1uZG4A+p1 LZHUA+qV1Y2xhAPqV
Y3MA+sVhZmFuYXN l dgd6nUtFWQD69WtZay0xMzg0MjM2MDA2APq9SUQtQ0VSVAD6
rf0cPhNsAAABogPiAoWU0fhDW54BCBo67GDaQVzzATzOZ2y l i+d9RaFHLdNjxAAC
urUFKBw+c20AAeIB6vL6nW5kbgD6nWVkdQD6pXVjbGEA+pVjcwD6xWFmYW5hc2V2
APqdS0VZAPr1a3NrL TEz0DQyMzYwMDYA+r1JRC1DRVJUAAAAAABmhiNMI l BfTAi
GA8yMDEzMTExMjAwMDAwMfoYDzIwMzMXMTEyMDAwMDAwWjAxMC8GA1UEKRMoL25k
bi9lZHUvdWNSYS9jcy9hZmFuYXNldi9rc2stMTM4NDIzNjAwNjJCCASlWdQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBAMTxeZ2GyHKQzBLV5iHwzJoGNG5c/uconE+
4yDXRFVwiHoAwtDfeL9psV732EkfbJqrN04V70TT55u54LPV5zUD3WDjR4T3KVcm
JBjC3K+CALUMs5a+Pp63ILQYrP/lX+4n1Ik6fUgeESQ233YKpEkM8u+CZLY6yEfo
Sb/0K7UsfQ/mE4YsPeOgOHZsuBxu7yMae5i lyR0t6ILCP4I5+XcV34mW94rIuMSX
OARqAIYfZ0zAfvCN7PMIwnGntrovpcIulfvVe//Dr9vHdegvKxa6DNE+QpN5FXh4
50Qjb6kkPbcBD3zQeUDT3opqkpUxhfeyeQKwHXioXHLB5HUsDYUCAwEAAQAA
[cawka@cawka-mac ~]$
```

NDN Certifications » Named Data Networking

ndncert.named-data.net/cert-req... Reader

Full Name:
Alexander Afanasyev

Homepage URL:
http://lasr.cs.ucla.edu/afanasyev/index.html

Institutional Group Name (optional):
Internet Research Laboratory

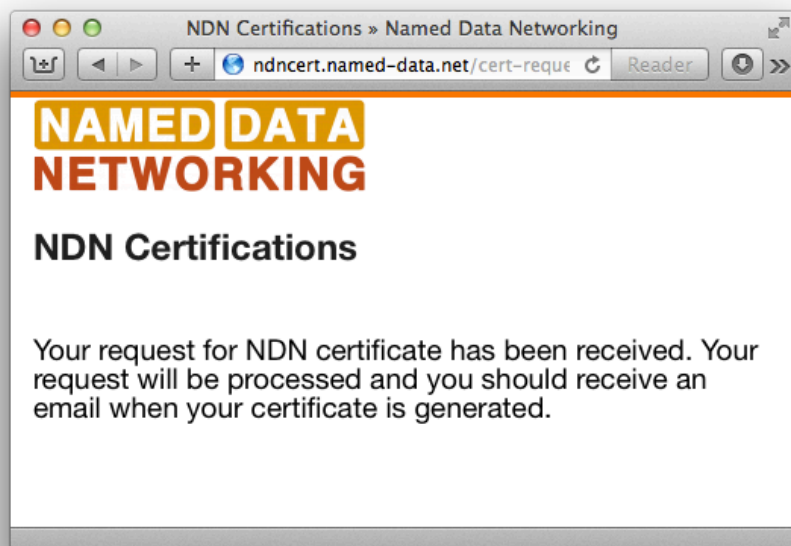
Advisor Name: (optional)
Lixia Zhang

NDN certification request

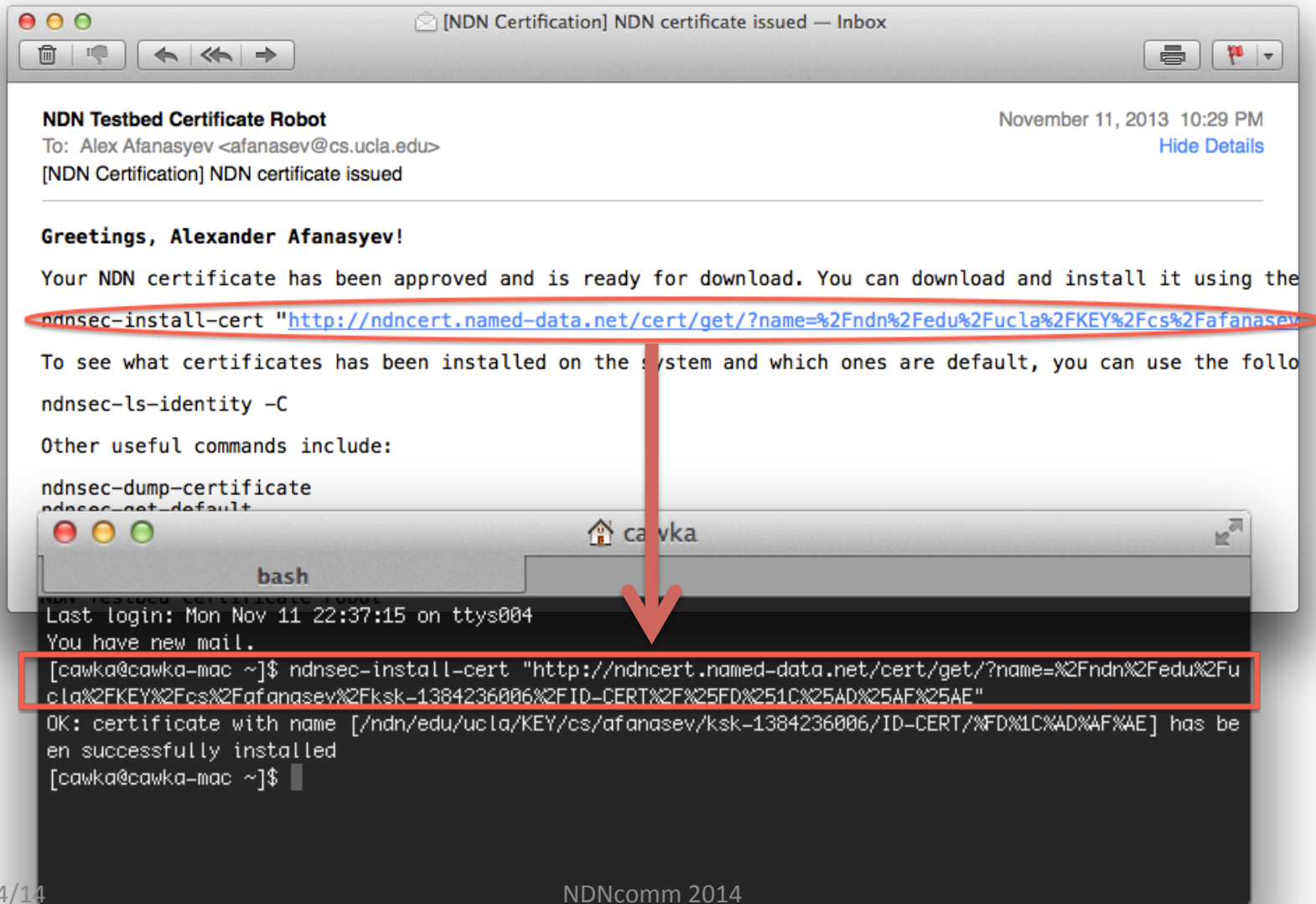
```
BIICqgOyEIW1HBOGIzCQS5qCaFGuXBYasDMvWm+pWuNMUA3IUDxiSrG8I5qxh+Vw
/UlZzNpsIRdGgTRpnxNVmvlP4vz/+xD1j7TGMRWiQ0xd6AbHaNVaBljYi09nqLnK
NhOXxPdEcTx9cIpYolWyQiZsbox0sP5LERM0lhzc0RfoxyVBozR+M4fLCQ7ufhd7
Ls6Ind+xcMNddNgND17h8QC7LyGHw9Ebl7NL4yOzA9uGVRCYHtY7hPu9HMqA+qBM
ZP/sm3lcizRvpgCKGqHuW9b8viqbTDzVjoU6VA/gf6foDevM6wK1eJ2gNgO+s8iK
FGPVS0J03TeFW+i1B3Xob6Lr8zVQapvZAADy+pluZG4A+pl1ZHUA+qV1Y2xhAPqV
Y3MA+sVhZmFuYXNldgd6nUtFWQD69WtZay0xMzg0MjM2MDA2APq9SUQtQ0VSVAD6
rf0cWjnlAAABogPiAoWU0fhDW54BCBo67GDaQVzzATzOZ2y l i+d9RaFHLdNjxAAC
urUFKBxaOcsAAeIB6vL6nW5kbgD6nWVkdQD6pXVjbGEA+pVjcwD6xWFmYW5hc2V2
APqdS0VZAPr1a3NrL TEz0DQyMzYwMDYA+r1JRC1DRVJUAAAAAABmhiNMI l BfTAi
GA8yMDEzMTExMjAwMDAwMfoYDzIwMzMXMTEyMDAwMDAwWjAxMC8GA1UEKRMoL25k
bi9lZHUvdWNSYS9jcy9hZmFuYXNldi9rc2stMTM4NDIzNjAwNjJCCASlWdQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBAMTxeZ2GyHKQzBLV5iHwzJoGNG5c/uconE+
4yDXRFVwiHoAwtDfeL9psV732EkfbJqrN04V70TT55u54LPV5zUD3WDjR4T3KVcm
JBjC3K+CALUMs5a+Pp63ILQYrP/lX+4n1Ik6fUgeESQ233YKpEkM8u+CZLY6yEfo
Sb/0K7UsfQ/mE4YsPeOgOHZsuBxu7yMae5i lyR0t6ILCP4I5+XcV34mW94rIuMSX
OARqAIYfZ0zAfvCN7PMIwnGntrovpcIulfvVe//Dr9vHdegvKxa6DNE+QpN5FXh4
50Qjb6kkPbcBD3zQeUDT3opqkpUxhfeyeQKwHXioXHLB5HUsDYUCAwEAAQAA
```

Submit
NDNComm 2014

5. Wait for the approval by the site's operator



6. Check mailbox and follow the instructions to install the issued certificate



The image shows a screenshot of an email and a terminal window. The email, titled "[NDN Certification] NDN certificate issued", is from the "NDN Testbed Certificate Robot" to Alex Afanasyev. It contains instructions on how to install the certificate using the `ndnsec-install-cert` command. A red circle highlights the URL in the email, and a red arrow points from it to the terminal window. The terminal window shows the command being executed and the successful installation of the certificate.

NDN Testbed Certificate Robot
To: Alex Afanasyev <afanasev@cs.ucla.edu>
[NDN Certification] NDN certificate issued
November 11, 2013 10:29 PM
[Hide Details](#)

Greetings, Alexander Afanasyev!

Your NDN certificate has been approved and is ready for download. You can download and install it using the `ndnsec-install-cert` "<http://ndncert.named-data.net/cert/get/?name=%2Fndn%2Fedu%2Fucla%2FKEY%2Fcs%2Fafanasev%2Fksk-1384236006%2FID-CERT%2F%25FD%251C%25AD%25AF%25AE>"

To see what certificates has been installed on the system and which ones are default, you can use the following command:

```
ndnsec-ls-identity -C
```

Other useful commands include:

```
ndnsec-dump-certificate
ndnsec-get-default
```

Terminal Window:

```
bash
Last login: Mon Nov 11 22:37:15 on ttys004
You have new mail.
[cawka@cawka-mac ~]$ ndnsec-install-cert "http://ndncert.named-data.net/cert/get/?name=%2Fndn%2Fedu%2Fucla%2FKEY%2Fcs%2Fafanasev%2Fksk-1384236006%2FID-CERT%2F%25FD%251C%25AD%25AF%25AE"
OK: certificate with name [/ndn/edu/ucla/KEY/cs/afanasev/ksk-1384236006/ID-CERT/%FD%1C%AD%AF%AE] has been successfully installed
[cawka@cawka-mac ~]$
```

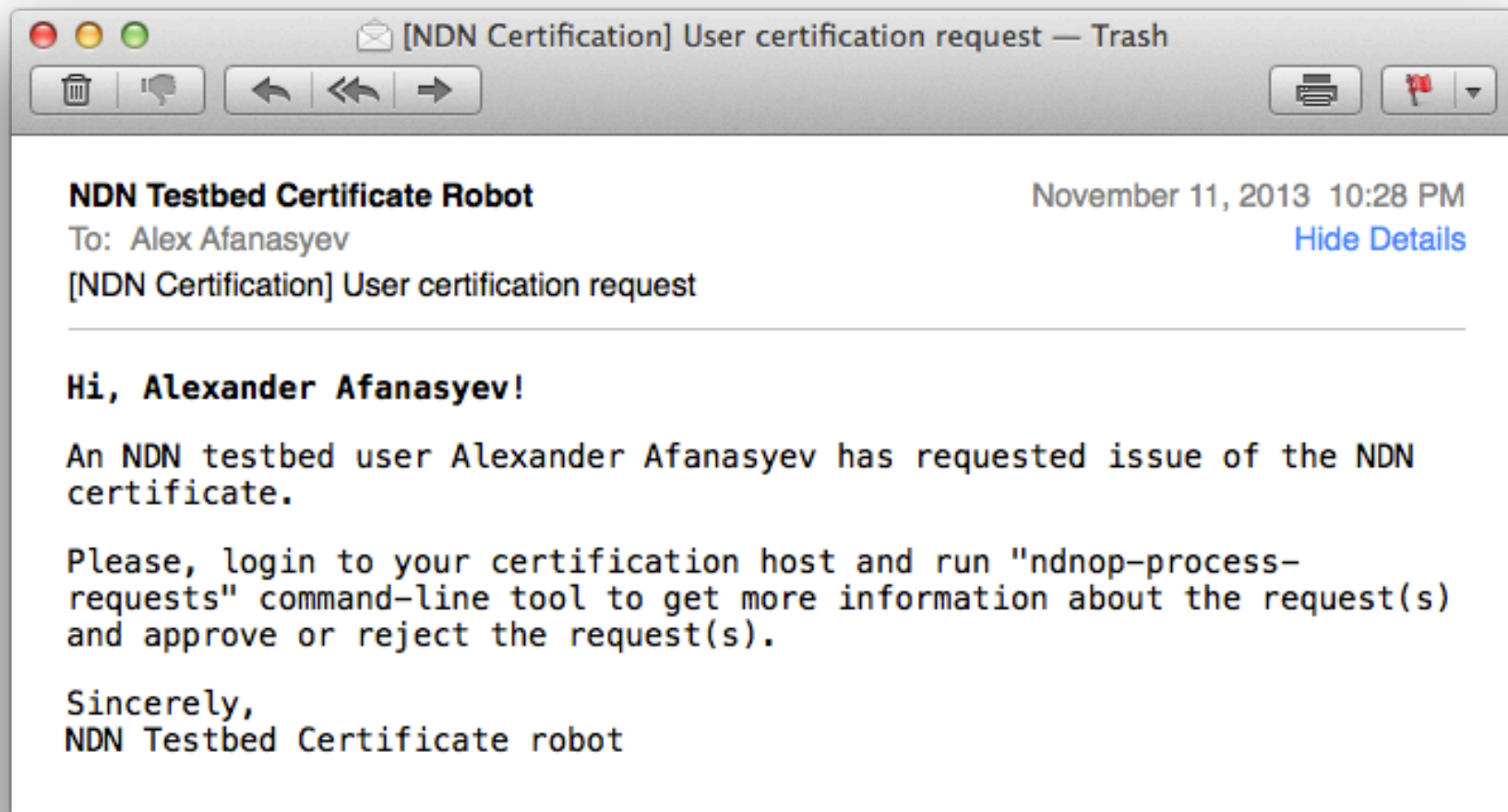
Congratulations

- You now have an NDN Testbed certificate for your public key
- ChronoChat is a first app that makes use of these certificates
 - <http://named-data.net/download/>

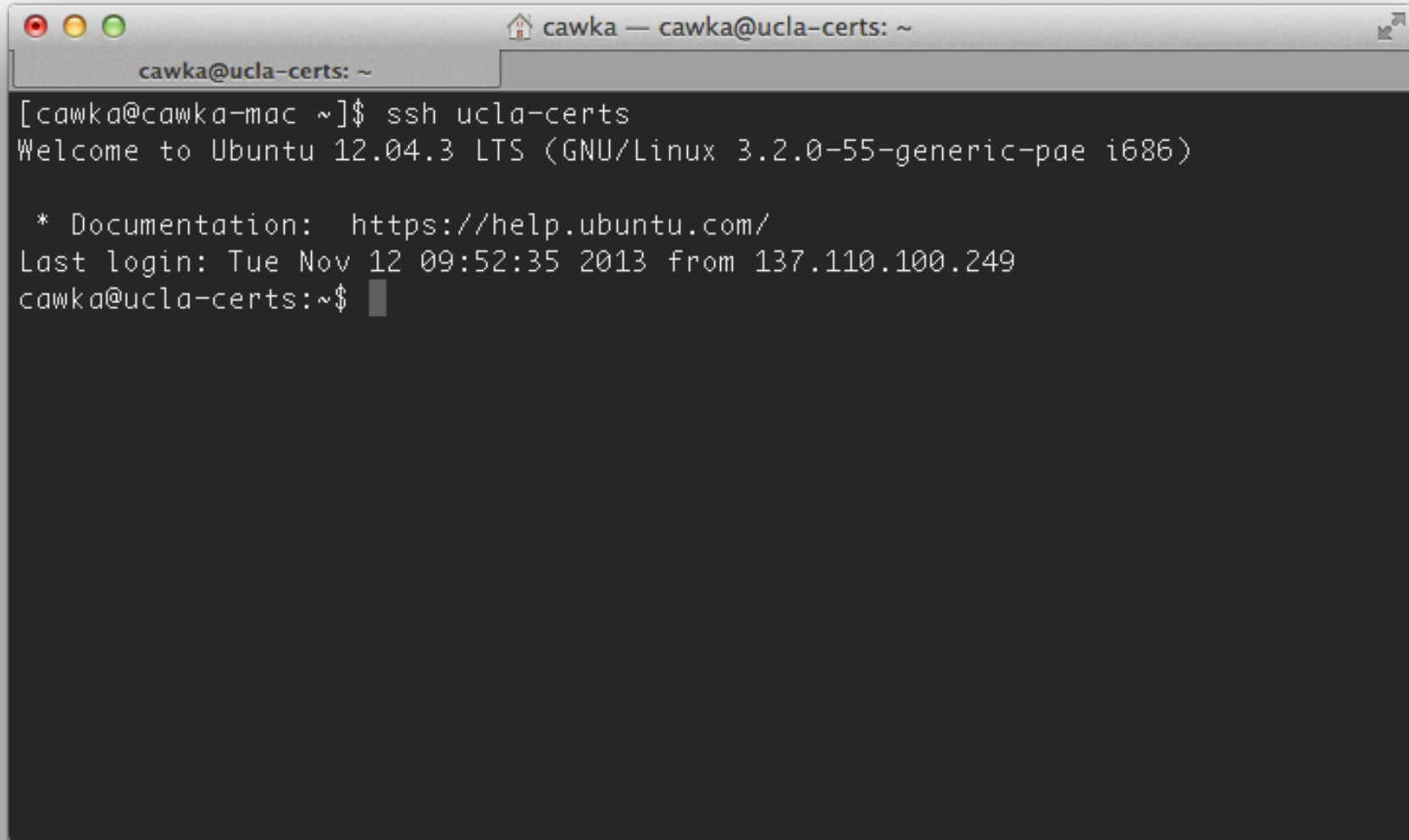
Operators guide

1. Wait for notification about users' certification request(s)
2. Log in (ssh) to the certification host
3. Run 'ndnop-process-requests' command and make decisions to approve/reject request

1. Wait for notification about users' certification request(s)



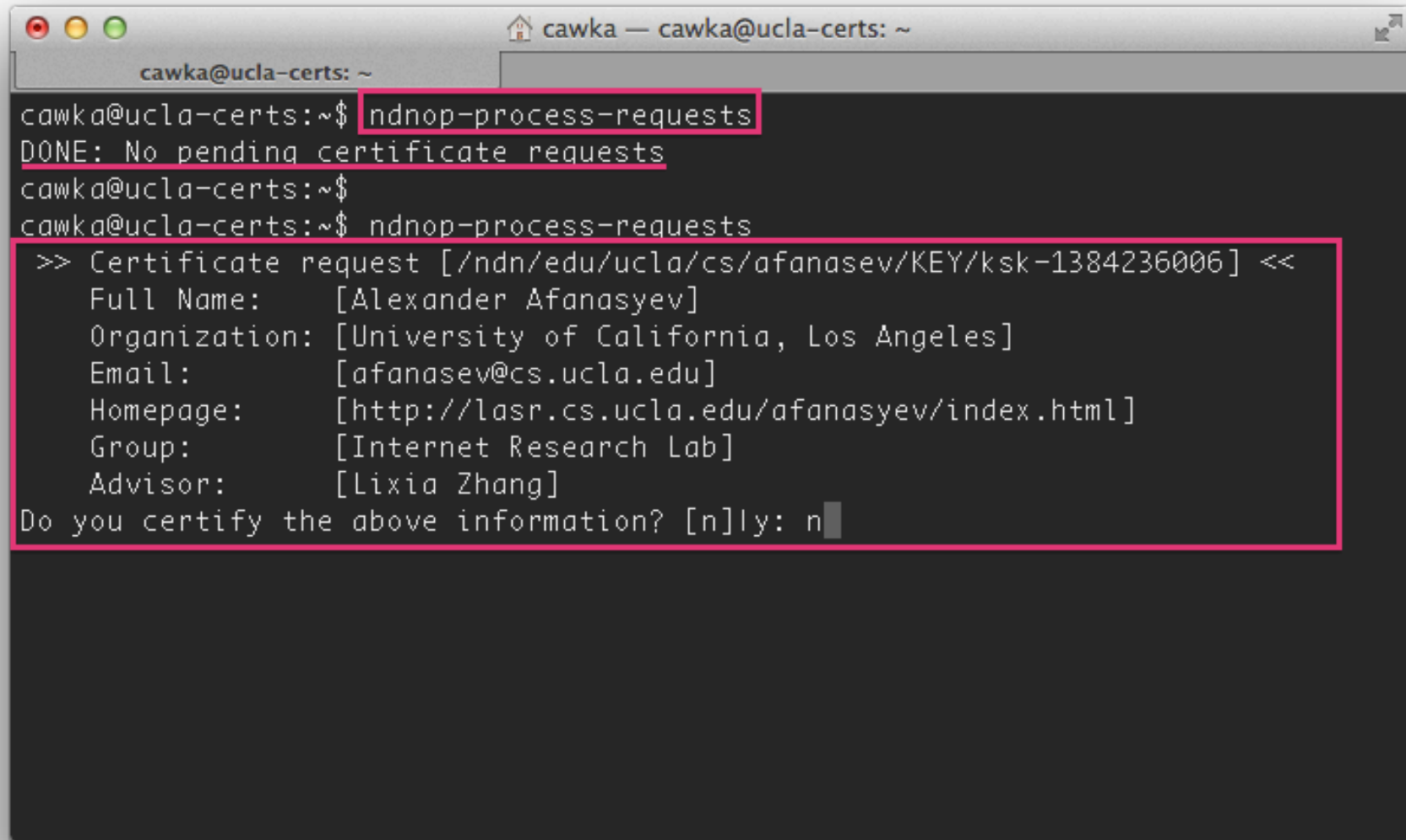
2. Log in (ssh) to the certification host

A terminal window titled "cawka — cawka@ucla-certs: ~" showing an SSH session. The user runs "ssh ucla-certs" from a local machine. The terminal displays the Ubuntu 12.04.3 LTS login banner, including the documentation URL and the last login time. The prompt then changes to "cawka@ucla-certs:~\$".

```
[cawka@cawka-mac ~]$ ssh ucla-certs
Welcome to Ubuntu 12.04.3 LTS (GNU/Linux 3.2.0-55-generic-pae i686)

 * Documentation:  https://help.ubuntu.com/
Last login: Tue Nov 12 09:52:35 2013 from 137.110.100.249
cawka@ucla-certs:~$
```

3. Run 'ndnop-process-requests' command and make decisions to approve/reject request



```
cawka@ucla-certs: ~  
cawka@ucla-certs:~$ ndnop-process-requests  
DONE: No pending certificate requests  
cawka@ucla-certs:~$  
cawka@ucla-certs:~$ ndnop-process-requests  
>> Certificate request [/ndn/edu/ucla/cs/afanasev/KEY/ksk-1384236006] <<  
Full Name: [Alexander Afanasyev]  
Organization: [University of California, Los Angeles]  
Email: [afanasev@cs.ucla.edu]  
Homepage: [http://lasr.cs.ucla.edu/afanasyev/index.html]  
Group: [Internet Research Lab]  
Advisor: [Lixia Zhang]  
Do you certify the above information? [n]ly: n
```


Current NDN Certificate Format

NDN Data packet

```
// NDN-TLV Encoding
Certificate ::= DATA-TLV TLV-LENGTH
    Name
    MetaInfo (=
CertificateMetaInfo)
    Content (= CertificateContent)
    Signature

CertificateMetaInfo ::= META-INFO-TYPE
    TLV-LENGTH
    ContentType (= KEY)
    FreshnessPeriod (= ?)

CertificateContent ::= CONTENT-TYPE
    TLV-LENGTH
    CertificateDerPayload
```

X.509-based Data packet content

```
// DER Encoding
CertificateDerPayload ::= SEQUENCE {
    validity      Validity,
    subject       Name,
    subjectPubKeyInfo SubjectPublicKeyInfo,
    extension     Extensions OPTIONAL }

Validity ::= SEQUENCE {
    notBefore     Time,
    notAfter      Time }

Time ::= CHOICE {
    GeneralizedTime }

Name ::= CHOICE {
    RDNSSequence }

RDNSSequence ::= SEQUENCE OF
    RelativeDistinguishedName

RelativeDistinguishedName ::=
    SET OF AttributeTypeAndValue

SubjectPublicKeyInfo ::= SEQUENCE {
    algorithm     AlgorithmIdentifier
    keybits       BIT STRING }

Extensions ::= SEQUENCE SIZE (1..MAX) OF
    Extension
```

[http://named-data.net/doc/ndn-cxx/
current/tutorials/security-library.html](http://named-data.net/doc/ndn-cxx/current/tutorials/security-library.html)

Open issues

- Current certificate model does not have “site’s operator” as part of certification chain
 - site operators collectively “own” site’s private key
- Certificate storage has limited infrastructure support
 - Currently using repo-ng
 - Plan to switch to NDNS as soon as it becomes available (~ October 2014)
- Limited revocation support
 - Currently based only on validity period