



Bundesministerium  
für Bildung  
und Forschung

# Grid computing, 基本的な環境

ATLAS ソフトウェア講習会 2016

河村 元

II.Physikalisches Institut, Universität Göttingen

# Overview

- Grid UI 環境
  - CERN の Lxplus と ICEPP のログインノード
  - おまけ： Docker による Grid UI
- Grid の基本概念
  - 概念
  - 認証局と VOMS

## Grid UI 環境



東京大学  
THE UNIVERSITY OF TOKYO



# CERN の Lxplus と ICEPP のログインノード

- lxplus

```
## If you have a CERN account  
ssh -Y YOUR_CERN_ACCOUNT@lxplus.cern.ch
```

- ICEPP UI

- <http://www.icepp.jp/howtouse.html>

```
## ICEPP login node (SL6)  
ssh -Y YOUR_ICEPP_ACCOUNT@login.icepp.jp
```

# おまけ： Docker による Grid UI (ラップトップなどで使用可能)

- In RedHat Enterprise 6 (CentOS, Scientific Linux)

## **## Installing Docker (as root)**

```
yum install docker-io
```

## **## You may need a permission (as root)**

```
chown root:dockerroot /var/run/docker.sock  
service docker start
```

## **## Check you are in docker group**

```
uid=500(gen) gid=500(gen) groups=500(gen),489(dockerroot)
```

## **## Make your Docker file**

```
cat Dockerfile
```

```
FROM binet/cvmfs-atlas
```

```
# Replace user, group, uid, gid by your user in a local PC
```

```
RUN export uid=500 gid=500 user=atlas001 group=atlas001 && groupadd $group -g $gid && useradd $user -u $uid -g $gid -d /home/$user -s /bin/bash
```

```
USER atlas001
```

```
ENV HOME /home/atlas001
```

## **## Building Docker container using CVMFS and ATLAS environments**

```
docker build -t atlas-ui .
```

## **## Running Docker container**

```
docker run -it -w /home/atlas001 -v $HOME:/home/atlas001 -v /tmp:/tmp atlas-ui /bin/bash
```

# Grid の基本概念



# 概念 - 1

- Grid はどのように動くのか？

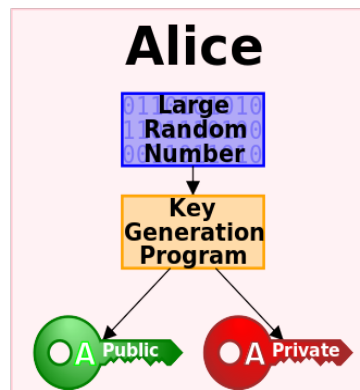
- 基本

- PKI（公開鍵認証インフラ）によるセキュリティ基盤
    - 同時に多人数のユーザーが利用
    - ユーザーの所属、実験等の識別
    - 計算資源のコントロール
    - ディスク資源やデータレプリケーションのコントロール
    - 世界中に分散した計算機の管理
    - ローカルな計算機のインターフェース
    - （例えば DNS のような）Tree 型の情報、計算資源検索
    - 末端ユーザーのためのツール（UI）



# 概念 - 2

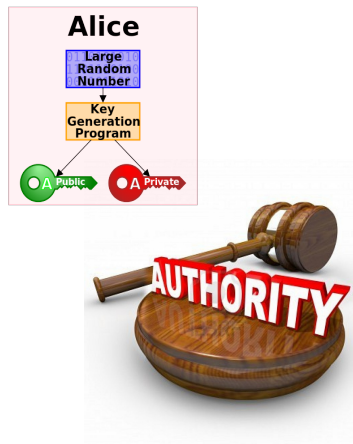
- User certificate, proxy certificate, CA, Virtual Organization (VO), VOMS, authentication, authorization
  - 証明書と認証メカニズム
    - ユーザー証明書の発行
      - 2つの巨大素数  $\rightarrow p$  and  $q$
      - 巨大な積  $N = pq$
      - 秘密鍵 (SK) に  $p + q$  を保存、 $N$  は公開鍵 (PK) として使用



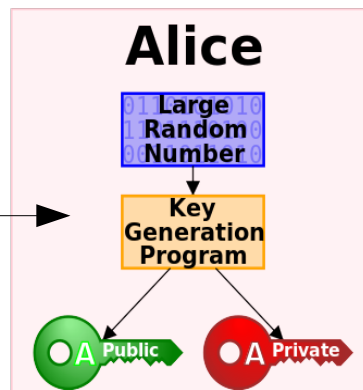


# 概念 - 3

- User certificate, proxy certificate, CA, Virtual Organization (VO), VOMS, authentication, authorization
  - 証明書と認証メカニズム
    - ユーザー証明書は CA によって署名される。
      - 署名 (S) はユーザー秘密鍵と公開鍵と文字列 X からタグ (T) 返す
      - 検証 (V) はユーザー公開鍵と X と T から 1/0 を返す。

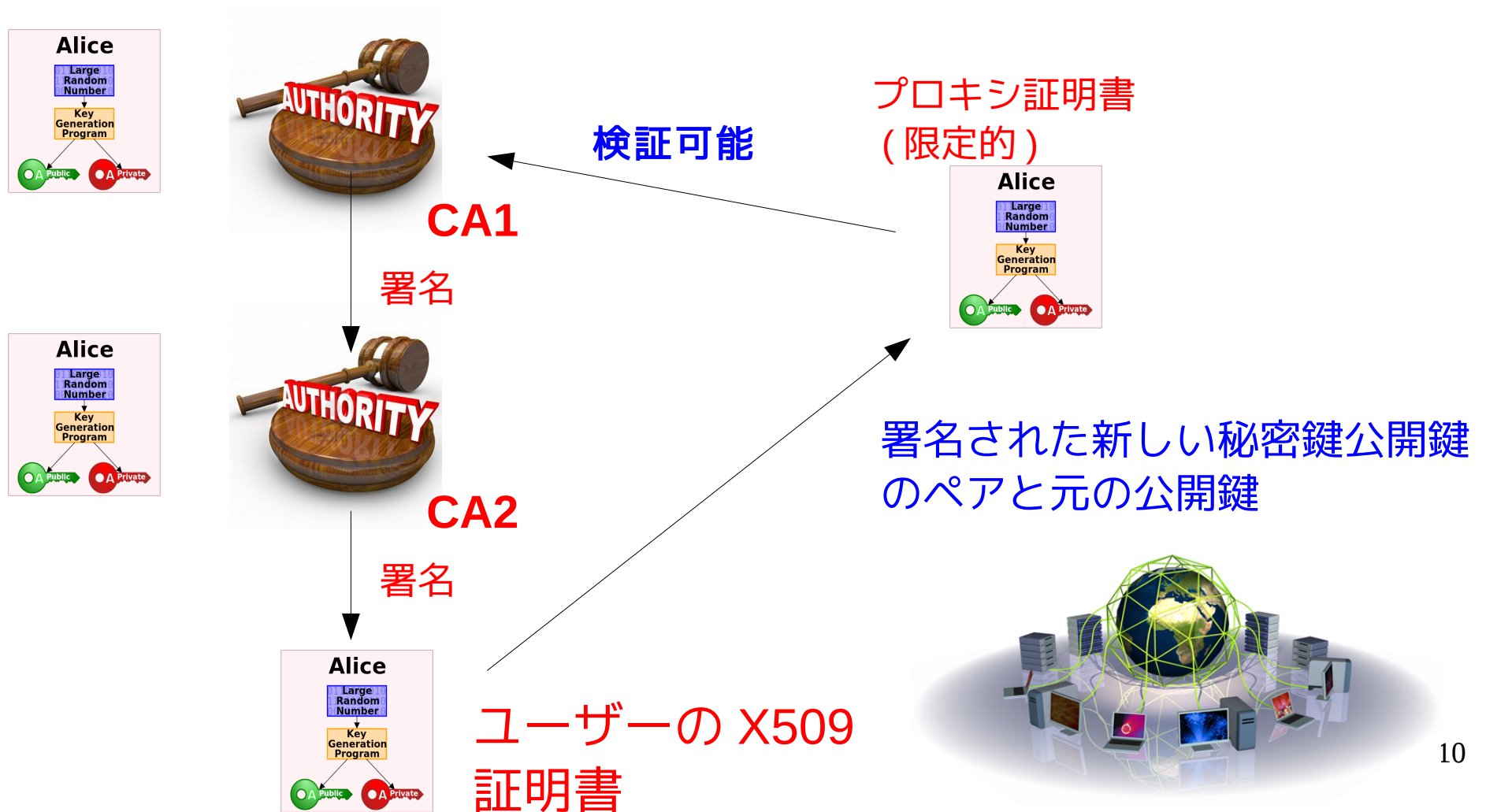


署名と検証



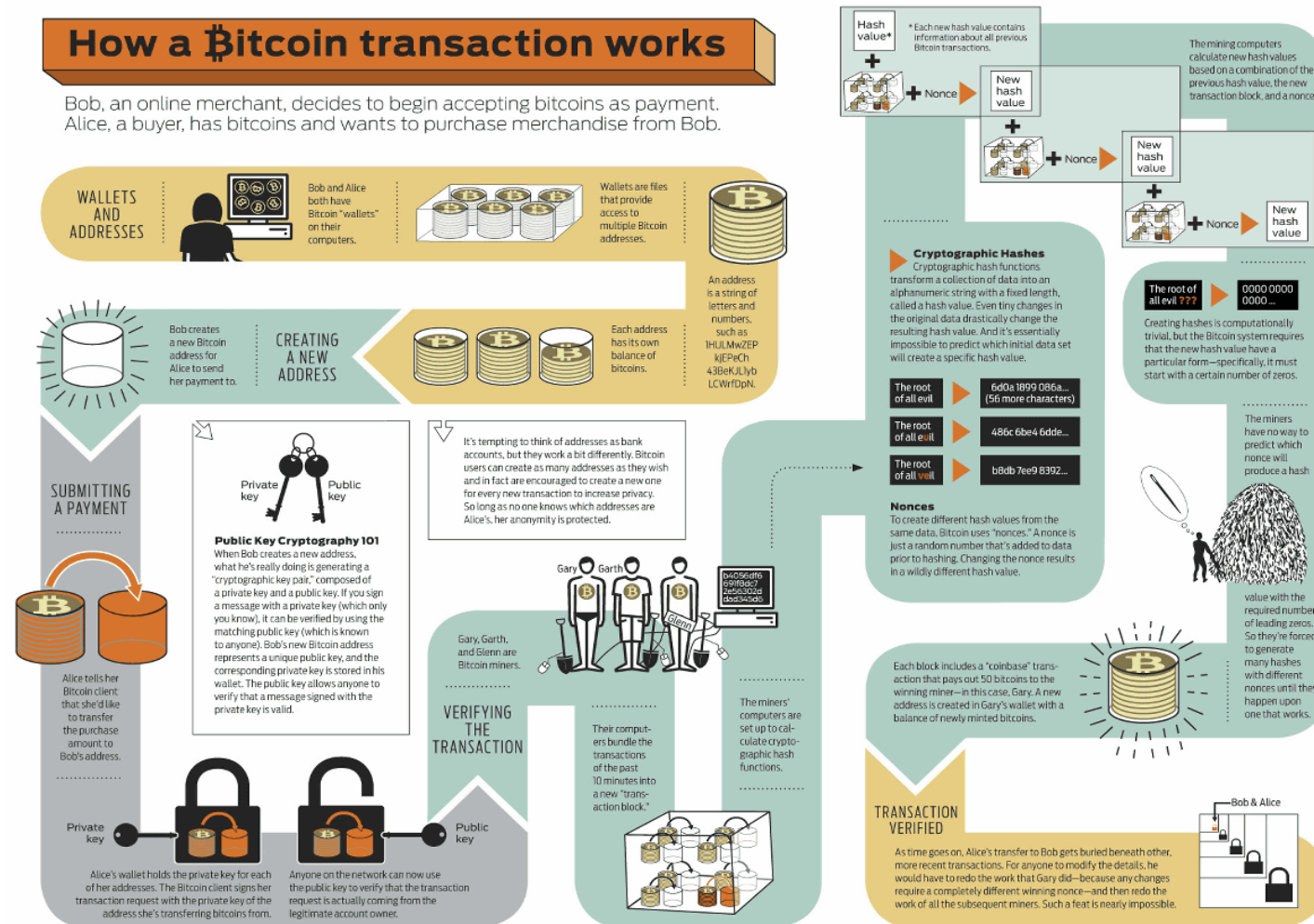
# 概念 - 4

- 新しい一時証明書の発行 = プロキシ証明書



# 実は良く似ています

- 全員認証局の証明書の無限連鎖（署名＝売買）
  - デジタル通貨 (Bitcoin)



# 概念 - 5

- Virtual Organization (VO), VOMS
  - VOMS 認証方式

認証局 (CA)



署名



署名



VO の要求  
voms-proy-init

ユーザー証明書

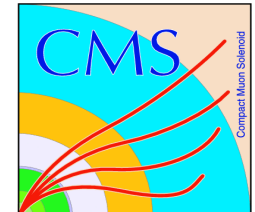
VOMS server

ATLAS VOMS  
CMS VOMS  
LHCb VOMS

VO 拡張フィールドの発行

プロキシ証明書  
= 限定された証明書

VOs



# 認証局と VOMS

- 日本 (KEK)

- <https://gridca.kek.jp/>
- 証明書の取得方法



Welcome to KEK GRID CA Web Repository

Web Enroll ( Only for Authorized Users )

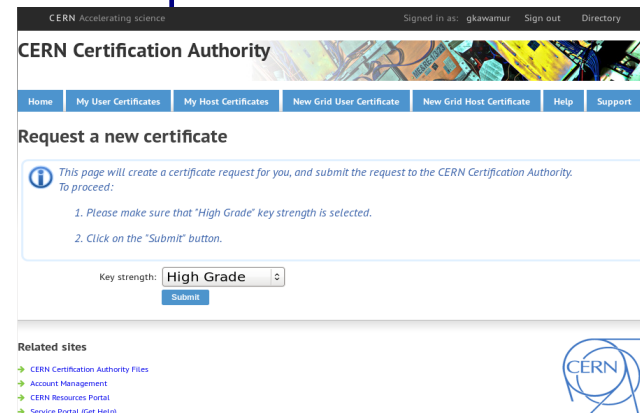
[Start Your Web Enrollment](#)

Documents

[User's Manual](#) | [Change History](#) | [CP/CPS](#)

- CERN

- <https://ca.cern.ch/ca/user/Request.aspx?template=EE2User>



# 認証局と VOMS

- VOMS top page
  - <https://voms2.cern.ch:8443/>
- VOMS ATLAS (ATLAS VO の要求 )
  - <https://voms2.cern.ch:8443/voms/atlas>
- VOMS ATLAS ユーザー
  - <https://voms2.cern.ch:8443/voms/atlas/services/VOMSCompatibility?method=getGridmapUsers&container=/atlas>



# リンクと参考文献

- Software twiki tutorial
  - <https://twiki.cern.ch/twiki/bin/viewauth/AtlasComputing/SoftwareTutorialGettingDatasets>
- Athena Docker setup
  - <https://twiki.cern.ch/twiki/bin/viewauth/AtlasComputing/AthenaMacDockerSetup>
- Docker container for CVMFS
  - <https://github.com/sbinet/docker-containers/tree/master/cvmfs-atlas>
- Binet, Sébastien, and Ben Couturier. "*docker & HEP: Containerization of applications for development, distribution and preservation.*" Journal of Physics: Conference Series. Vol. 664. No. 2. IOP Publishing, 2015.
  - <http://iopscience.iop.org/article/10.1088/1742-6596/664/2/022007/meta>
- Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008).
- ATLAS-D meeting 2016 Grid/Rucio Tutorial, Gen Kawamura
- Athena Mac Docker
  - <https://twiki.cern.ch/twiki/bin/viewauth/AtlasComputing/AthenaMacDockerSetup>
- ATLAS Software Tutorial, Feb 2016
  - <https://indico.cern.ch/event/465378/>



# Backup



# CVMFS の設定

- 個人的な好み
  - ~/.bashrc などを書いておくと便利

```
## Alias to initialization of VOMS proxy
alias vinit='voms-proxy-init --voms atlas -hours 200 --valid 200:00'

## Alias to setupCVMFS
setupCVMFS(){
  export LCG_LOCATION=
  export ATLAS_LOCAL_ROOT_BASE=/cvmfs/atlas.cern.ch/repo/ATLASLocalRootBase
  source $ATLAS_LOCAL_ROOT_BASE/user/atlasLocalSetup.sh ""

  ## Using EMI LCG package
  source ${ATLAS_LOCAL_ROOT_BASE}/packageSetups/atlasLocalEmiSetup.sh --emiVersion ${emiVersionVal}
}

setupATLAS(){
  export ATLAS_LOCAL_ROOT_BASE=/cvmfs/atlas.cern.ch/repo/ATLASLocalRootBase
  source $ATLAS_LOCAL_ROOT_BASE/user/atlasLocalSetup.sh ""
}

## Using CVMFS (with EMI LCG client tools)
SetupCVMFS

## Using ATLAS env
setupATLAS
```

# ユーザー証明書

- ユーザー証明書 (CERN の場合)

```
## Check important environment variables for your certificate  
env | grep X509
```

```
## Generating a proxy certificate  
export X509_USER_CERT=~/.globus/usercert.pem  
export X509_USER_KEY=~/.globus/userkey.pem
```

```
## Generate user certificate  
## (usercert.p12 was already exported by your browser)  
openssl pkcs12 -clcerts -nokeys -in usercert.p12 -out $X509_USER_CERT
```

```
## create a private certificate with passphrase  
openssl pkcs12 -nocerts -in usercert.p12 -out $X509_USER_KEY
```

```
## Set permissions  
chmod 644 $X509_USER_CERT  
chmod 400 $X509_USER_KEY
```

```
## show enddate  
openssl x509 -in $X509_USER_CERT -noout -enddate
```

```
## show if the certificate is valid  
openssl verify -CApath $X509_CERT_DIR -purpose sslclient $X509_USER_CERT
```

# プロキシ証明書

- プロキシ証明書と簡単な検証

## **## Generating a proxy**

**vinit**

Enter GRID pass phrase for this identity:

Contacting voms2.cern.ch:15001 [/DC=ch/DC=cern/OU=computers/CN=voms2.cern.ch] "atlas"...

Remote VOMS server contacted succesfully.

voms2.cern.ch:15001: The validity of this VOMS AC in your proxy is shortened to 345600 seconds!

## **## Generating a proxy certificate without VO**

**grid-proxy-init**

**voms-proxy-info -all**

# (it displays information without VO attributes)

## **## Generating a proxy certificate with VO (a normal use)**

**voms-proxy-init --voms atlas -hours 200**

**voms-proxy-info -all**

# (it displays information with VO attributes)

## **## Using another role (if you have another)**

**voms-proxy-init -voms atlas:/atlas/de/Role=production**

**voms-proxy-info -all**

# プロキシ証明書の検証

- 中身を見てみましょう

```
## Check context of your certificate
## The proxy certificate has 3 fields (PK, New PK, New SK)
less /tmp/x509up_u$UID | grep '\-'

-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----

## Check X509 attribute
openssl x509 -in /tmp/x509up_u$UID -text | less

## Using a different proxy certificate
## (switch them if you have several ones)
mv -v /tmp/x509up_u$UID /tmp/x509_different_cert
export X509_USER_PROXY=/tmp/x509_different_cert
voms-proxy-info -all
```