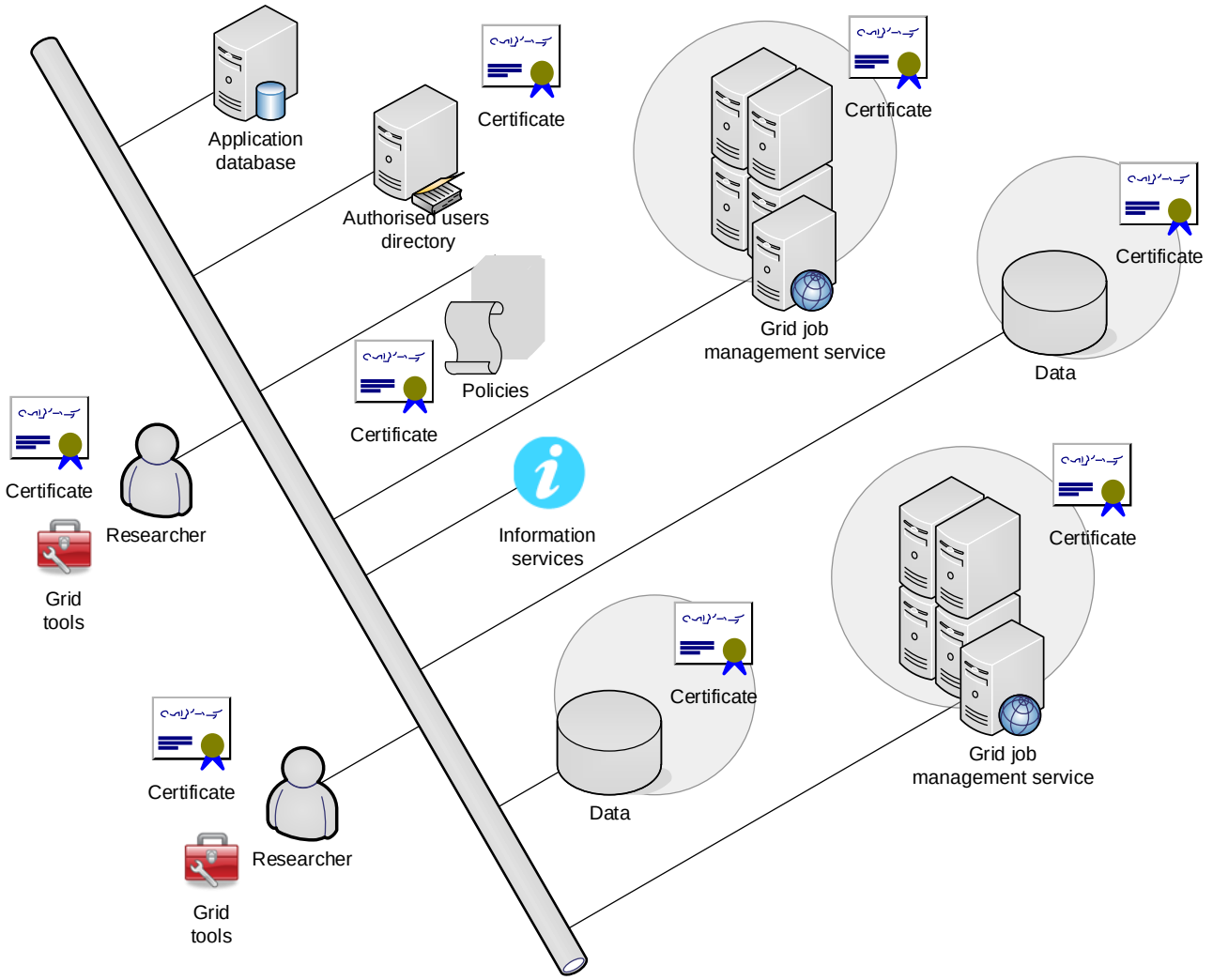
Security and certificates

From one cluster to many: Grid

- Recall: you used password to access the cluster
- You also had a personal user space (account)
- Now scale it up 100+ clusters and 1000+ users
  - You can't quite remember 100+ passwords
  - Sysadmins can't quite manage 1000+ user accounts
- Solution: use Public-Key Infrastructure (PKI)
  - Each user has a digital certificate
  - Each service also has a certificate

Every Grid actor is certified

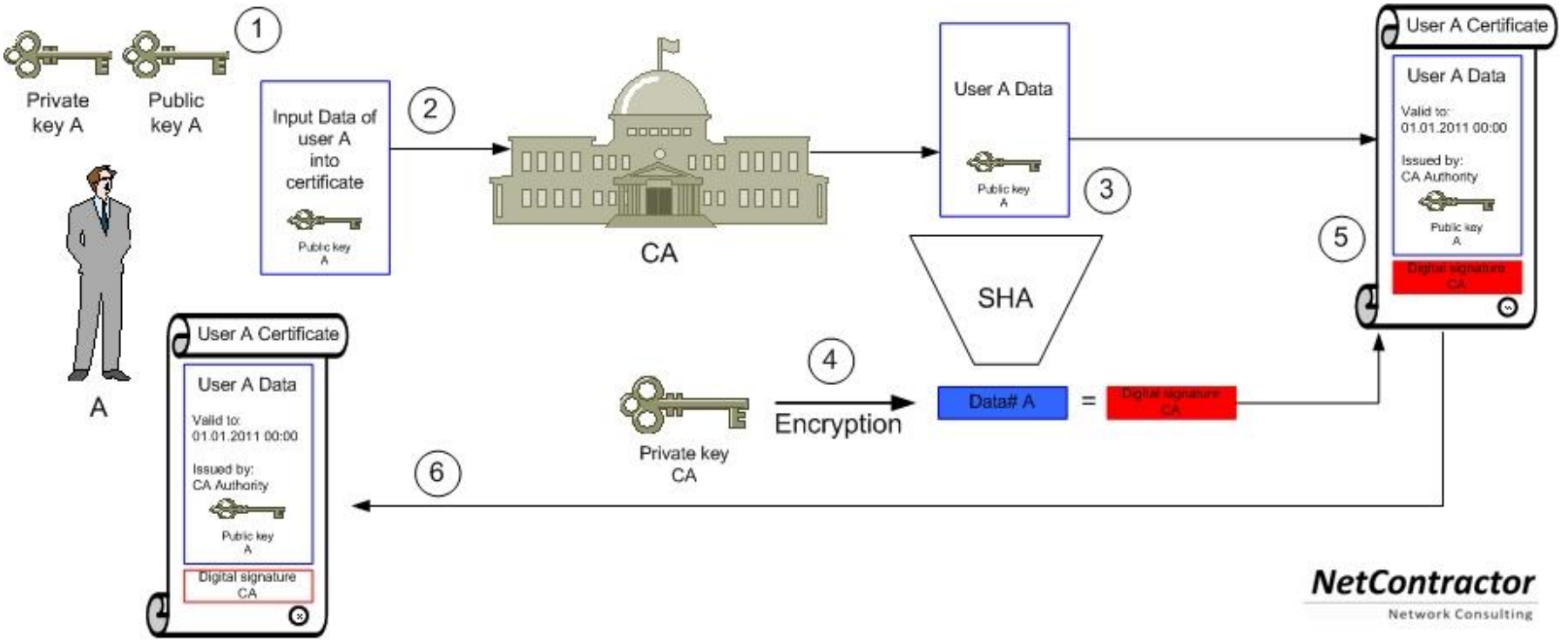


LUND UNIVERSITY

Principles of PKI

- Goals:
  - reliably verify identity of users and authenticity of services by means of digital signatures
  - communicate securely over public networks
- There are trusted Certificate Authorities (CA) that can vouch for:
  - identities of users
  - trustworthiness of services
- Each actor (user, service, CA) has a public-private pair of keys
  - Private keys are kept off-line; public keys are shared
  - Keys are used for both authentication and communication encryption/decryption
    - » For our purposes, authentication is most important
- CAs digitally sign public certificates of eligible users and services
  - Public certificate contains owner information and their public key
  - Each CA has a set of policies to define eligibility

Obtaining a personal certificate



Beware: words “certificate” and “key” are often used interchangeably!

LUND UNIVERSITY

Private key

- Private key is a cryptographic key – essentially, a sufficiently long random number
  - Longer it is, more difficult it is to crack; 2048 bit is good (as of today)
- Purposes:
  - Create digital signature
  - Decrypt encoded information
- There are many softwares that create private keys
  - Even your browser can do it
  - Keys come in many different formats
- **Important**: private key must never travel over public unprotected network
  - Don't store it in Dropbox!

Public key

- Mathematically linked to the private key
  - It should be impossible to derive private key from the public one
    - » Different public-key algorithms exist
    - » Benefit: no need to securely exchange private keys, as public keys are enough and can travel unprotected
- Purposes:
  - Verify owner's digital signature
  - Encrypt plain information
- Usually, software tools create public and private key in one go
  - They can even be stored in one file

LUND UNIVERSITY

Protocols using public key cryptography

- Some examples:
  - SSH
  - SSL and TLS (used e.g. in https, Gmail)
  - GridFTP: a variant of FTP tailored for Grid
  - PGP and GPG (used e.g. to sign software packages or sign/encrypt e-mail)
  - Bitcoin
  - ZRTP (used by secure VoIP)

Grid flavour of PKI

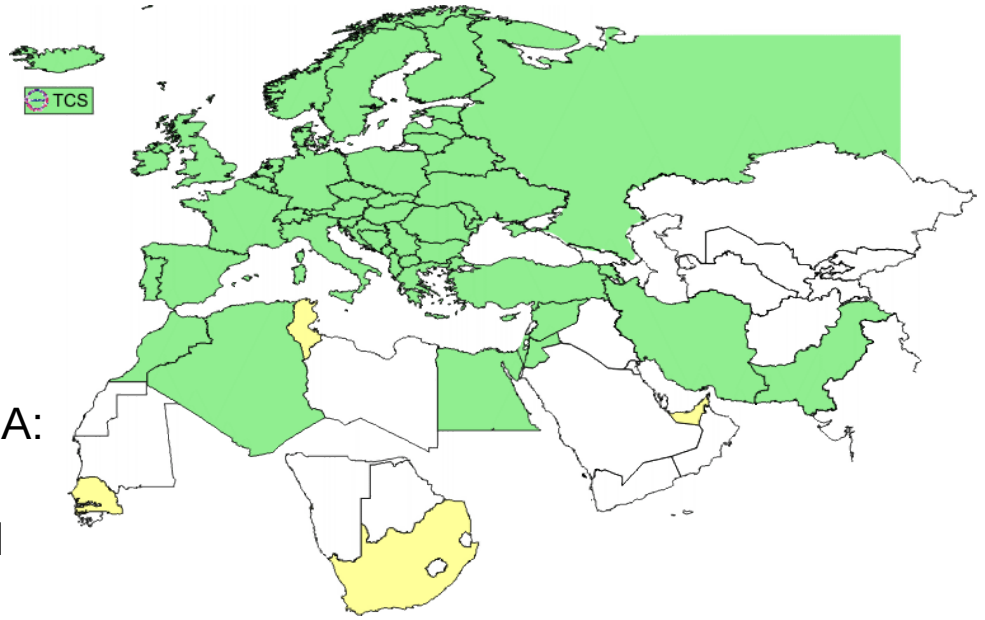
- Historically, Grid makes use of the **X.509** PKI standard
  - Defines public certificate format
    - » Certificate must include subject's Distinguished Name (DN)
    - » Certificate has limited validity period
  - Assumes strict hierarchy of trusted CAs
    - » Unlike PGP, where anyone can vouch for anyone
    - » Check your browser for pre-defined list of root CAs
  - Requires certificate revocation status checks
  - Certificate is password-protected
    - » You can not reset the password; if forgotten, a new certificate must be requested
- One can convert X.509 certificates into SSH ones

Certificate Authorities

- Web browsers and even operating systems come with a set of trusted root CA certificates
  - You can always add own trusted CAs, or remove untrusted ones
    - When you remove a CA, you won't be able to securely connect to a server certified by that CA
- Grid has an own set of trusted CAs: the International Grid Trust Federation (**IGTF**)
  - http://www.igtf.net/
- In order to use Grid, you **must** keep the IGTF CA certificates up-to-date!
  - Several releases per year
  - Each CA is represented by a separate package
    - One can uninstall an untrusted CA
  - Packages are available from IGTF and two Grid projects: EGI, NorduGrid
    - RPM, deb, tar

IGTF

- European part of IGTF: EUGridPMA
  - https://www.eugridpma.org/
- Each country used to have an own CA
  - CERN also has a CA
  - Nordic countries have one CA
- Nowadays, there is a single European CA: TERENA
  - TERENA is a federation of national research network providers
  - Relies on national network operators to confirm identities
  - National operators rely on universities and such



You still need all the IGTF CA certificates!

LUND UNIVERSITY

Certificate revocation lists (CRL)

- Certificates of people and services can be revoked
  - If they are compromised, or if some information in the certificate is changed
    - » If your affiliation changes, you must get a new certificate, and the old one must be revoked
- For security reason, before connecting to a service, software must check whether its certificate is revoked or no
- Certificate revocation lists (CRLs) are published by CAs
  - They are regularly updated
  - You must regularly refresh your local copy of CRLs
    - » A cron-based tool exist
- Other technologies exist – e.g. Online Certificate Status Protocol (OCSP) – but in the Grid world CRLs rule

Mutual authentication

- Authentication is establishing validity of person's (or service) identity
  - Not to be confused with authorisation: established identity may still lead to denied access
- Users and services on the Grid must mutually authenticate
  - Both parties must have valid certificates
  - Both parties must trust the CAs that signed each other's certificates
    - » "Trusting a CA" means having the CA's public certificate stored in a dedicated folder/store
    - » Removing a CA certificate breaks trust
    - » Removing your own signing CA certificate breaks everything
- Technically, authentication process involves exchange of encrypted messages, which parties can decrypt only if they are who they claim to be

From theory to practice

- Before doing anything on the Grid, you will need to obtain:
  - IGTF CA certificates
    - » Packages include CRLs
    - » Regular updates for CRL and IGTF packages must be in place
  - Private key and public certificate
    - » Grid uses PEM encoding for keys and certificates (ASCII)
    - » Typical file names: **`userkey.pem`** and **`usercert.pem`**
    - » Note: public key is inside the CA-signed certificate **`usercert.pem`**
  - PKCS#12 formatted certificate containing private and public keys, as well as CA signature and CRL info
    - » PKCS#12 certificate (.p12) is used mostly by browsers, but can also replace PEM files in some Grid tools
    - » One can extract PEM files from PKCS#12 one, and other way around

How to create a certificate

The easy way:

- Google for TERENA e-Science portal
- Log in using your university credentials
- Follow the instructions
- The certificate in PKCS#12 format will be stored in your browser certificate store
- You can export the certificate into a file (.p12) and extract PEM files, if necessary

How does it work:

Browser creates private and public keys for you

Public key is sent to TERENA CA, along with information that University provides about you

Signed public certificate is returned back to your browser, and merged with the private key to create a PKCS#12 certificate

LUND UNIVERSITY

Other ways to create certificates

- Use **`grid-cert-request`** tool from the Globus Toolkit
  - Make sure you install all the IGTF CA packages
  - For Nordic countries, install package **`ca_NorduGrid-certrequest-config`** from the NorduGrid CA
    - » http://ca.nordugrid.org
    - » For other countries, check your CA instructions
  - Executing **`grid-cert-request`** will create the PEM-encoded key pair; the public key must be sent to your CA for signing
- You can be your own CA, or use so-called Instant CA tools
  - Of course, this will fall outside the Grid trust perimeter

Summary: why use certificates?

- Certificates are your digital passports
  - Contain the necessary information (in particular, Distinguished Name)
  - Are signed by trusted authorities, verifying your identity
  - Are used to authenticate access requests originating from you
- Certificates are used in authorisation
  - Grid services can authorise a list of Distinguished Names
    - » No need to create user-specific accounts
  - The only password you need to remember is the one of your certificate
- Services are also certified
  - Enables secure interactions
  - You need all the IGTF CA certificates to access all services on the Grid

Exercises

- Inspect root CA certificates
  - trusted on the system-level (e.g. **`/etc/ssl/certs, /etc/pki, /usr/share)`**
  - trusted in your personal browser profile: Firefox/Chrome/MSIE
- Get TERENA certificate (see the corresponding slide)
  - Find the Terena CA portal (google terena escience certificate), login with your LUCAT id
  - Request a new certificate via generating a Certificate Signing Request (CSR) in the browser
  - Install the certificate into your browser (save in keystore)
  - Download your certificate from the browser's keystore in PKCS#12 format (open the certification manager and "backup" your Terena certificate), save it as e.g. cert.p12
- Extract private and public keys from the cert.p12 "bundle format" using **`openssl`** command
  - **`openssl pkcs12 -nocerts -in cert.p12 -out userkey.pem`**
  - **`chmod 400 userkey.pem`** (private key always must be protected)
  - **`openssl pkcs12 -clcerts -nokeys -in cert.p12 -out usercert.pem`**

Exercises

- Explore your certificate files with **`openssl`** (both the .p12 and .pem formats)
  - **`openssl x509 -in usercert.pem -subject -issuer -dates -noout`**
  - **`openssl pkcs12 -info –in cert.p12`**
- Explore/establish trust relation within the Grid world:
  - Explore the pre-installed CA files in **`/etc/grid-security/certificates, e.g.`** check if TERENA one is there
  - Check CRLs (NorduGrid CA in this example):
    `openssl crl -in /etc/grid-security/certificates/1f0e8352.r0 –text | less`
- Check for the latest IGTF updates, install (trust) “experimental” CAs
  - Fetch the latest IGTF distribution as a single package (google “igtf bundle”)
  - Follow the README and use the proper configure options to Install the selected CA files under your personal trusted CA certs location
- Backup your certificate(s) and cleanup the desktops
  - Don’t forget to copy your personal .pem and .p12 files to your USB key
  - Remove all copies of your certificates from the login machine including the browser ‘s keystores!