




# ArmeSFo – EUGridPMA initiative for implementation of PKI in NATO Partner and Mediterranean Dialogue Countries

**Ara Grigoryan[1], David Groep[2], Arsen Hayrapetyan[1]**

*[1]Armenian e-Science Foundation, 49 Komitas Ave, 0051 Yerevan, Armenia*
*[2]DutchGrid and NIKHEF CA, Kruislaan 409, 1098 SJ, P.O. Box 41882 NL 1009 DB, Amsterdam, Netherlands*

*aagrigor@mail.yerphi.am, davidg@nikhef.nl, ahairape@mail.yerphi.am*

**Third int. Conference "Grid technologies and distributed computing in science and education"**
**30 June - 4 July 2008, Dubna, Russia**

# Contents

- Security requirements to information in Cyberspace
- Public Key Infrastructure (PKI) - modern approach to secure the information
- International Grid Trust Federation
- PKI statistics on NATO – allied and partner countries
- ArmeSFo – EUGridPMA Initiative

# Security of information in Cyberspace

**Security requirements to the information in cyberspace involve:**

- **Authentication of end-entities (EEs), users/clients, computers/servers and services → Knowledge of the information origin/sender**
- **Integrity → Proof that the information was not altered or forged during its transfer**
- **Confidentiality → Hiding the information content from unwanted parties**
- **Non-repudiation → In dispute cases, preventing a sender of information to repudiate, or refute the validity of information**

# Public Key Infrastructure

**A worldwide accepted standard meeting these security requirements is Public Key Infrastructure (PKI)**

**PKI = asymmetric crypto-technique + Certification Authority (CA)**

**With asymmetric crypto-technique, a key pair (public and private keys) is generated for EEs**

**CA signs (with its private key) the public key of EE and issues the EE's public key certificate (or simply certificate). The certificate binds the public key with EE identity.**

**The EE identity is unique for each CA.**

**The EE identity, the public key, their binding, validity conditions and other attributes are made unforgeable in the certificates issued by CA.**

# PKI in action

## PKI technologies meet all security requirements

- **Authentication of EEs:** Sender signs with its private key the information to be sent. Authenticity of the sender is verified by other EEs using the sender's certificate and CA root certificate(s)
- **Confidentiality and privacy:** Information is encrypted with public key of the recipient. Only recipient can decrypt the message using its private key
- **Integrity of information transferred between the authenticated EEs:** Is implicitly provided by authentication procedure
- **Non-repudiation:** Is assured by digital signature of sender

# Regional PMAs and IGTF

**There exists a worldwide network of national Academic CAs, issuing certificates for the national and international collaborations. These CAs are united in three regional organisations – Policy Management Authorities (PMAs):**

**European Grid PMA (EUGridPMA)** ***http://www.eugridpma.orgl*****,**

**The Americas Grid PMA (TAGPMA)** ***http://www.tagpma.orgl*****,**

**Asia Pacific Grid PMA (APGridPMA)** ***http://www.apgridpma.orgl***

**The largest of them, EUGridPMA, unites CAs from 44 countries and organisations**

**The PMAs are joined in International Grid Trust Federation (IGTF)** ***http://www.gridpma.orgl*** **– a body to establish common policies and guidelines between PMAs**

# Regional PMAs and IGTF

**The certificates issued by CAs from regional PMAs allow specialists to work in the international e-Science and Grid projects aimed at the collaborative investigations in many areas of human activity: medicine, biology, Earth science, physics, engineering, etc.**

## Conclusion to this state-in-the-art part:

**It becomes more and more evident that the implementation of security-providing PKI technologies in a country is one of the preconditions of the country's effective involvement in the international intellectual activity.**

# NATO - related PKI statistics

***green - has CA, red - no CA, grey – preparations to establish CA***

**NATO 26 countries**

**Belgium, Bulgaria, Canada, Czech Republic, Denmark, Estonia, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Luxembourg, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Turkey, United Kingdom, United States**

**Partner 23 countries**

**Albania, Armenia, Austria, Azerbaijan, Belarus, Bosnia and Herzegovina, Croatia, Finland, Georgia, Ireland, Kazakhstan, Kyrgyz Republic, Moldova, Montenegro, Russian Federation, Serbia, Sweden, Switzerland, Tajikistan, the former Yugoslav Republic of Macedonia, Turkmenistan, Ukraine, Uzbekistan**

**Mediterranean Dialogue 7 countries**

**Algeria, Egypt, Israel, Mauritania, Morocco, Jordan, Tunisia**

**19 countries out of 56 are not spanned by PKI**

# Another, NATO – specific view

**Virtual Silk Highway (a large NATO project) countries**

**Armenia, Azerbaijan, Georgia, Kazakhstan, Kyrgyz Republic, Tajikistan, Turkmenistan, Uzbekistan, Afghanistan**

**Mediterranean Dialogue countries**

**Algeria, Egypt, Israel, Mauritania, Morocco, Jordan, Tunisia**

**Other European Partner countries that have no CA**

**Albania, Belarus, Bosnia and Herzegovina, Moldova, Montenegro**


BELARUS
UKRAINE
MOLDOVA
KAZAKHSTAN
Lake Balkhash
Aral Sea
GEORGIA
ARMENIA
AZERBAIJAN
Yerevan
UZBEKISTAN
KYRGYZSTAN
TURKMENISTAN
TAJIKISTAN
AFGHANISTAN
TUNISIA
MOROCCO
ALGERIA
MAURITANIA
ISRAEL
JORDAN
EGYPT

# PKI implementation Programme

**At the ICS panel meeting of September 2007, Ara Grigoryan (member of Information and Communications Security (ICS) advisory panel of NATO SPS Programme), presented the Programmeof Implementation of PKI in the countries that have no CAs.**

**In January 2008, the Programme was presented by Arsen Hayrapetyan (manager of ArmeSFo CA) at the EUGridPMA meeting.**

**The Programme was discussed in detail and approved by both organisations.**

# PKI implementation Programme

**The Programme will be conducted on stage-by-stage basis.**

**Stage 1: Creation of standard software toolkit for CA operations, template *Certificate Policy and Certification Practice Statement* as well as detailed documentation on CA routine.**

**The corresponding Collaborative Linkage Grant project *'Adapting Public Key Infrastructure software for improved Cybersecurity in Partner countries'* *co-directed by UK e-Science CA manager Jens Jensen and ArmeSFo CA manager Arsen Hayrapetyan* was submitted to the ICS panel, approved and awarded.**

# PKI implementation Programme (cont)

**Stage 2:** **Second stage is foreseen as NATO Advanced Networking Workshop in Armenia with participation of the representatives of EUGridPMA, and ICT specialists from the target countries–future national CA managers. The Workshop will include lectures on PKI, presentation of the created CA toolkit and accompanying documentation, practical courses on the work with toolkit. It is assumed that the trainees will get necessary background to establish national CAs and apply for the accreditation at EUGridPMA. The application for a NATO grant is under preparation.**

**The necessity of further stages will depend on the outcome of the Workshop.**

## The project is ambitious: 15 ‘no-PKI’ countries will be involved

### Problems

- **Extreme diversity of the ICT level in the countries**
- **Insufficient knowledge of English in some countries. (Minimum) national language support will be needed**
- **Psychological problems. Understanding of the necessity of the Project**
- **Relations between the involved countries**

**Involvement of Russian PKI specialists is important!**

**ArmeSFo invites Russian colleagues to discuss how they can be involved in the conduction of the Project. ArmeSFo will be happy to invite interested Russian PKI experts to participate with their contribution in the Workshop.**

# Thank you for your attention!