PKI for improved cybersecurity in NATO Partner countries

Software

Arsen Hayrapetyan, **ArmeSFo CA**

Beginning of the project

- Idea of the project originated in 2007 by Ara Grigoryan, ArmeSFo CA Manager
- Presented at NATO Information and Communication Security Panel meeting in September 2007, Istanbul, Turkey
- Presented and discussed at 12th EUGridPMA meeting in Amsterdam, The Netherlands, in January 2008
- Received the approval and support of the PMA
- Applied for NATO collaborative linkage grant (CLG) in January 2008
- CLG awarded in June 2008
- Principal investigators and co-directors
  - from NATO country: Jens Jensen (UK)
  - from NATO partner country: Arsen Hayrapetyan (Armenia)

Goals of the project

- Provide target countries of the project (next slide) with tools for deploying PKI as means of improving the level of cybersecurity
  - Establishing CAs
  - Contribute to their integration into EUGridPMA

- To achieve these goals, the target countries should be provided with:
  - Software for CA operations
  - Policy guidelines

Target countries

- **Countries along the Virtual Silk Highway (large networking project under NATO funding since 1994):**

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

- **Mediterranean Dialogue countries**

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

-- do have CA

-- do not have CA

Software requirements

- The software should allow
  - Easy deployment on both Windows and Linux
  - Support for all CA operations required by off-line classic CA
  - Easy configuration of CA root and EE certificates in accordance with IGTF standards
    - Provide default configuration conforming to Grid Certificate Profile (GCP)
  - Adding new features seamlessly and without extra effort (posed by the software itself)

Software choice

- Initially planned to use OpenCA and adapt it to IGTF standards
- Abandoned the idea of using OpenCA. Instead, own software is being developed. The software will be owned by EUGridPMA

Advantages of using own soft (1)

- Own software is designed with off-line CAs and IGTF standards in mind. It does not have OpenCA's extra (and potentially confusing or not-easy-to-configure) features
- The software is being coded in PHP. Many PMA experts are experienced in PHP (more than in perl?), so they could contribute easily to the future versions of software
- The software is modular, it has the "core" part and uses SOAP to communicate with other modules performing specific tasks (signing CSR, issuing CRL, etc.). Specific modules can be implemented in any language supporting SOAP communications

Advantages of using own soft (2)

- Software is IGTF standards-centered. It should allow issuing GCP-compliant certificates, as well as support mechanisms for updating the configuration to match possible changes of GCP
- Software will be owned by PMA and can be modified or branched at any time without depending on third-party owner

What kind of CAs is the software for?

We expect target countries to be off-line CAs with one or more RAs, with no subordinate CAs.

- The software will provide interfaces for
  - CA operations
  - RA operations
  - User operations

Supported configuration

- The software is meant to be installed on two machines:
  - offline (CA offline machine), for CA operations like signing certificates, issuing CRLs, etc.
  - online
    - interface for users to request, renew and revoke their certificates, etc.
    - interface for RAs, to approve or reject certificates, etc.
    - Interface for CA to publish CP/CPS, CRLs, send automatic notifications, etc.

CA operations (offline)

- Support for following operations:
  - Generation of CA key pair and certificate
  - Issuing EE certificates (X.509 v3)
  - Revoking certificates
  - Issuing CRLs (v1 & v2)
  - Configuring certificate profiles
  - Backup operations (making backup, CA recovery using backup, etc.)

CA operations (online)

- Support for following operations:
  - Publishing CP/CPS, CRLs, other public info
  - Sending automatic notifications about certificate expiration to certificate holders
  - DB lookup operations

RA operations

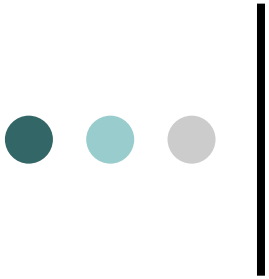
- Support for following operations
  - Approving or rejecting requests
  - Requesting revocation of certificates
  - DB lookup operations

User operations

- Requesting certificates
- Renewing certificates
- Requesting revocation of own certificate
- Verifying status of own certificate

GCP compliancy

- Support for a default EE certificate profile compliant with GCP
- Support for importing the profile (the form is not decided yet, e.g. XML) managed centrally (e.g. EUGridPMA repository)
  - Application of GCP changes quickly
  - Staying up-to-date with IGTF requirements to EE certificate profile



Comments, suggestions…?