

Securing Access to Greek e-Gov Services

Konstantinos Rantos (MSc, PhD)
General Secretariat of Public Administration
and E-Government
Hellenic Ministry of Interior

4th Regional Information Security Forum
Thessaloniki, November 2008

AGENDA

- ▶ Introducing Greek e-gov services
- ▶ Digital Authentication Framework
- ▶ “Syzefxis” PKI and lessons learned
- ▶ Hermes
- ▶ European aspects

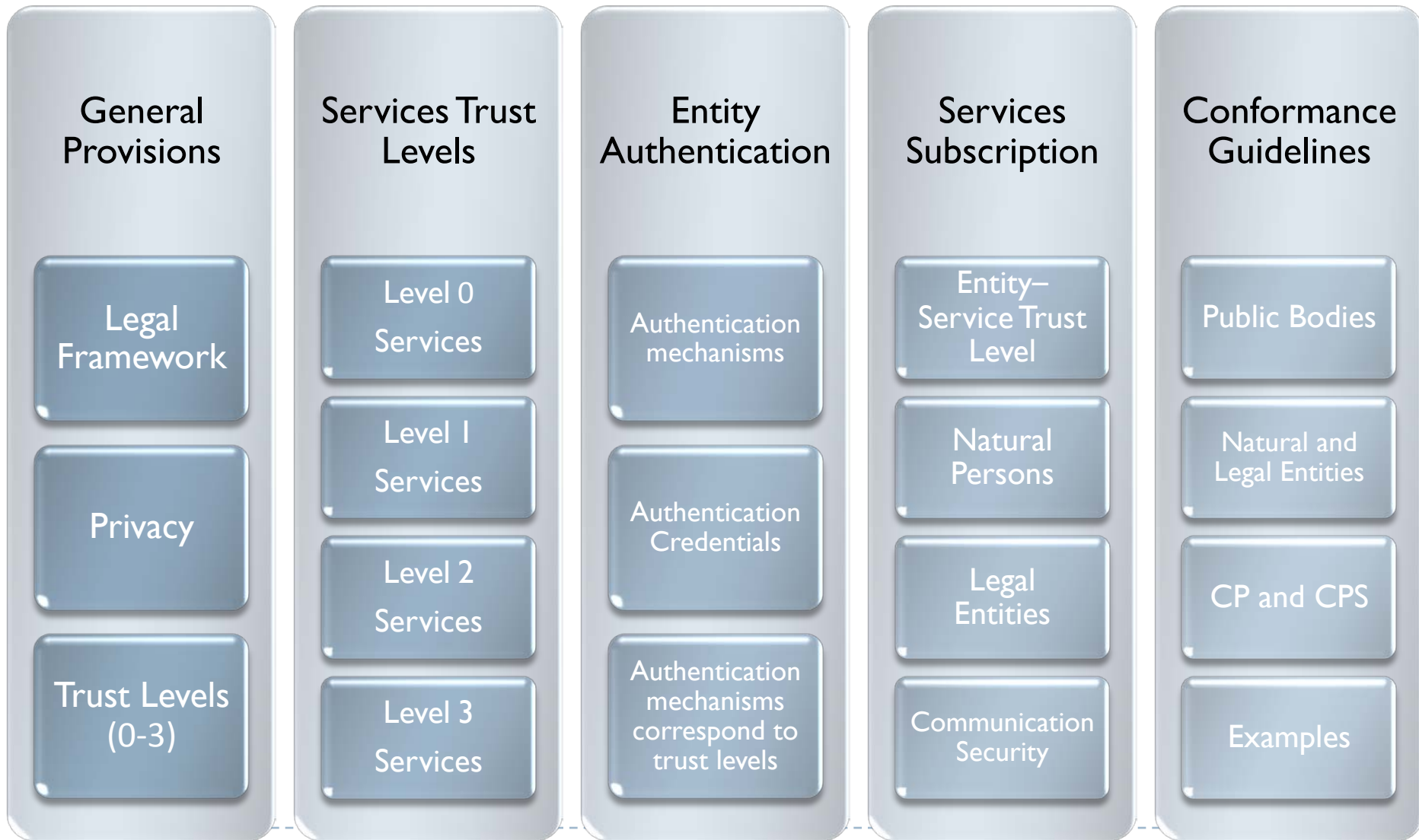
Hermes Portal

- ▶ Provision of e-gov services
- ▶ One stop shop
- ▶ Single sign-on
- ▶ In conformance with the
Greek e-Government Interoperability Framework

Greek e-GIF

- ▶ Provides guidelines for implementing e-gov services
 - ▶ Interoperability and Electronic Services Provisioning Framework
 - ▶ Certification Framework for Public Administration Sites and Portals
 - ▶ **Digital Authentication Framework**
 - ▶ Documentation Model for Public Administration Processes and Data
 - ▶ Interoperability Registry prototype

Authentication Framework



“Syzefxis” PKI

- ▶ Established in the context of the Greek Public Administration Network
- ▶ Provides certification services to all public servants
 - ▶ Qualified Electronic Signature
 - ▶ Encryption
- ▶ Enables
 - ▶ Replacement of handwritten signatures
 - ▶ Secure document and email exchange
 - ▶ Secure system access



Lessons learned by “Syzefxis”

- ▶ Lack of compulsory use was a burden
- ▶ Legal framework exists; procedures were not defined though
- ▶ Registration should be simplified (without relaxing security)
- ▶ Transparent use is important
- ▶ Education

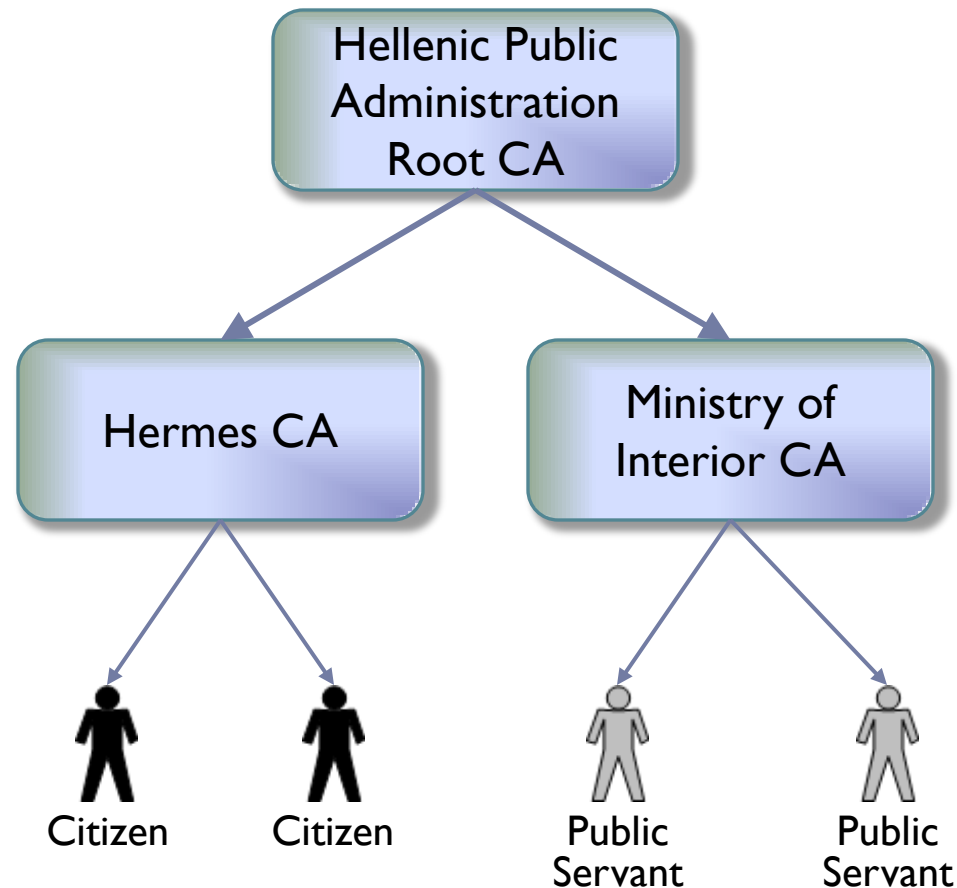
Hermes authentication model

- ▶ Username – Password
- ▶ Soft Certificates
- ▶ Certificates stored on SSCD

- ▶ Authentication mechanism depends on provided service
 - ▶ Stronger mechanisms can be used for lower trust levels

HERMES CA

- ▶ Part of the Hellenic Public Administration Infrastructure



Hellenic Public Administration Infrastructure

▶ Certificate Policies

- ▶ Qualified Electronic Signatures + Authentication (Private Keys reside on SSCD)
 - ▶ Advanced Electronic Signature based on Qualified Certificate (no SSCD)
 - ▶ Sectoral Authentication Certificate
 - ▶ Encryption Certificate
- ▶ Certificates are issued only to natural persons
- ▶ Conformance to standards and Greek as well as European Legal Framework
- ▶ ETSI 101 456
 - ▶ ETSI 101 862
 - ▶ PD 150/2001 (EU Directive on Electronic Signatures)
 - ▶ Hellenic Communications and Post Commission Decisions

Typical Use

► Certificates Issued to a Citizen

Digital Signature

Subject DN

- Country
- Common Name
- Surname
- Given Name
- Serial Number

Names are also in Greek

Email is optional

Encryption

Subject DN

- Country
- Common Name
- Surname
- Given Name
- Serial Number

Names are also in Greek

Email is optional

Sectoral Authentication

Subject DN

- Country
- Common Name
- Surname
- Given Name
- Serial Number

Subject Alternative Name

- Sectoral ID (encrypted)

Sectoral Authentication and Serial Number

- ▶ Lack of unique id assigned to citizens + Data Protection Law restrictions
 - ▶ No id can be included in the certificate
- ▶ Serial Number (Certificate Administration Code)
 - ▶ It is not an id
 - ▶ Same for all certificates issued to a citizen by a CSP
 - ▶ Guarantees uniqueness of names
 - ▶ Facilitates certificate management

European Aspects

- ▶ Hermes does not accept foreign ids (at this stage)
- ▶ Can I use my certificate to access other Member States' e-gov services and exchange signed documents?
 - ▶ Is HERMES CA recognized across EU members?
 - ▶ Are the certificates issued by HERMES accepted by Member States?
- ▶ There is work under development at European Level
 - ▶ Services Directive
 - ▶ Issuance of Trusted Lists by supervisory bodies

Konstantinos Rantos

Informatics Development Agency
General Secretariat of Public Administration and E-Government
Hellenic Ministry of Interior

k.ran@yap.gov.gr

www.yap.gov.gr

www.gspa.gr

