The policy of the Bulgarian Government in the field of Network and Information Security

Author: Assoc. Prof. Slavcho Manolov, PhD –
Advisor to the Chairman of SAITC,
Alternate member of ENISA Management Board

ITU Regional CyberSecurity Forum (Sofia, 7-9.09.2008)

The Electronic Governance Act

The e-Governance Act has been adopted by Bulgarian Parliament on 12.06.2007. It regulates the functioning of administrative bodies in circumstances of electronic documents exchange and electronic administrative services provision.

The Law contains special chapter devoted to the information security, which clearly regulates the requirements in this field for administrations and their information systems.

In the same chapter the Law specifies the public authority responsible for the development and implementation of information security policy, including the exercise of control - the State Agency for Information Technology and Communications.

Special attention to the Network and Information Security

Unlike the hitherto prevailing practice of autonomous development of information systems in each administration, the requirements of the law for a single input of data from citizens and businesses need to produce intensive information exchange between administrative systems. This creates a new type of threats:

- Transfer of vulnerability from one system to another;
- Blocking the electronic services of a system where poor availability of another, etc.

Therefore the achievement of a certain acceptable level in network and information security of all systems becomes a requirement for their interaction.

Inclusion in upcoming systems for provision of pan-European cross-border electronic services is also associated with this condition.

The Regulation on general requirements for Information Security

This document is one of the six sub-legal acts, which complements and specifies the requirements of the law. The Regulation and its 13 annexes formulate both the policy and the specific requirements for network and information security in the administrative information systems.

The governmental policy defined in the Regulation contains measures for network and information security management, which can be realized at two levels: central level and the level of administrative body.

Besides the investigation of national experts, the policy development was based on the study of IBM for infrastructure of the Bulgarian administration as well as consultations with ENISA.

Two levels of the governmental policy

1. The central level includes the following measures :

1.1. Establishment and centralized management of the National electronic communications network (NESM) under methodological control of SAITC;

1.2. Establishment of National Computer Security Incident Response Team (N-CSIRT);

1.3. Creation of Unified environment for secure exchange of electronic documents (ESOD);

1.4. Implementation of the National e-Governance Data Model for Public Administration through centrally managed Registers for Unified Primary Metadata;

1.5. Conducting of unified policy on Disaster Recovery Centers;

1.6. Establishment of Central unit for monitoring of network and information security under SAITC.

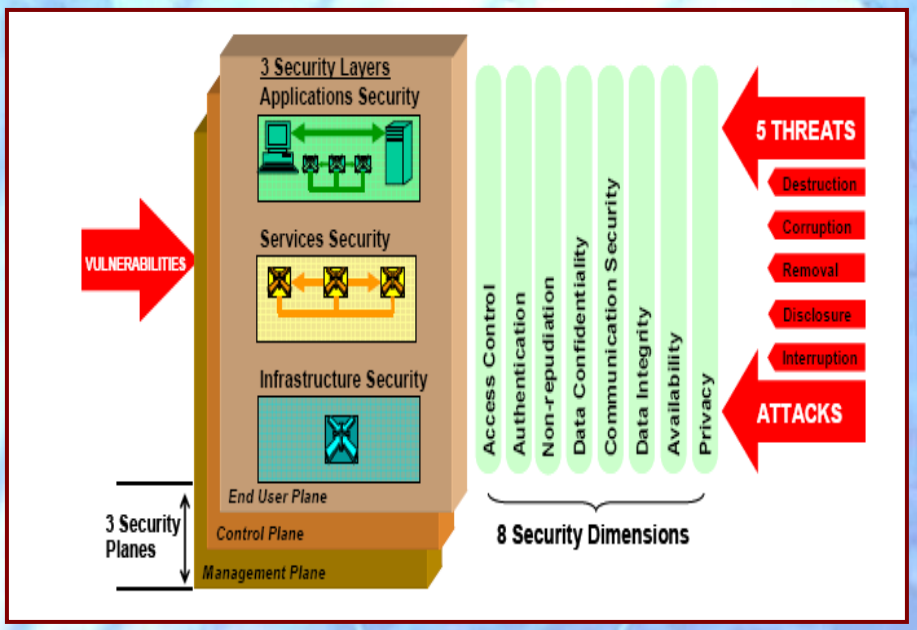
2. The level of administrative body is based on:

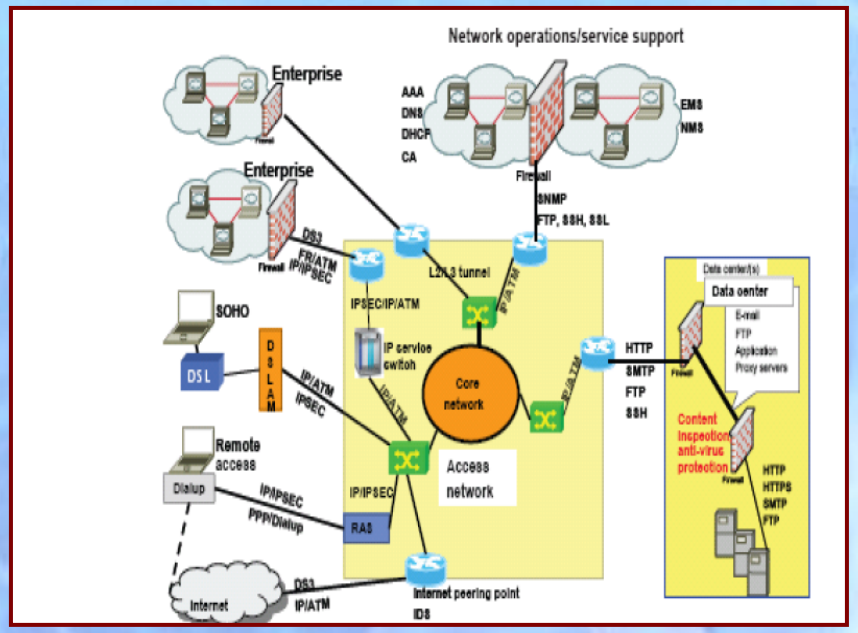
2.1. Internal rules along the lines of "the systems of information security management", regulated by ISO 27001:2005;

2.2. Specific certification of administrative information systems in accordance with Chapter Six of the Regulation.

National Telecommunication Network

The guaranteed network and information security in the telecommunications processes can be ensured only by a closed network with central management of the services and a few highly controllable gateways to the surrounding world. Following the Regulation, the central network administrator will be responsible for implementing the measures for network security in accordance with the ITU recommendations H.800 and H.805, including the Internet-protection.

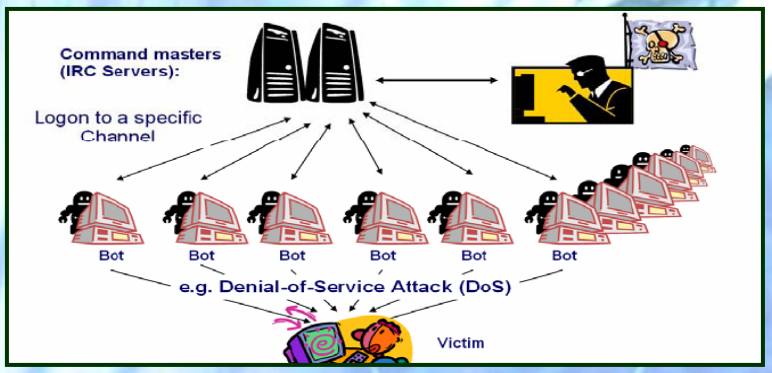




National Computer Security Incident Response Team

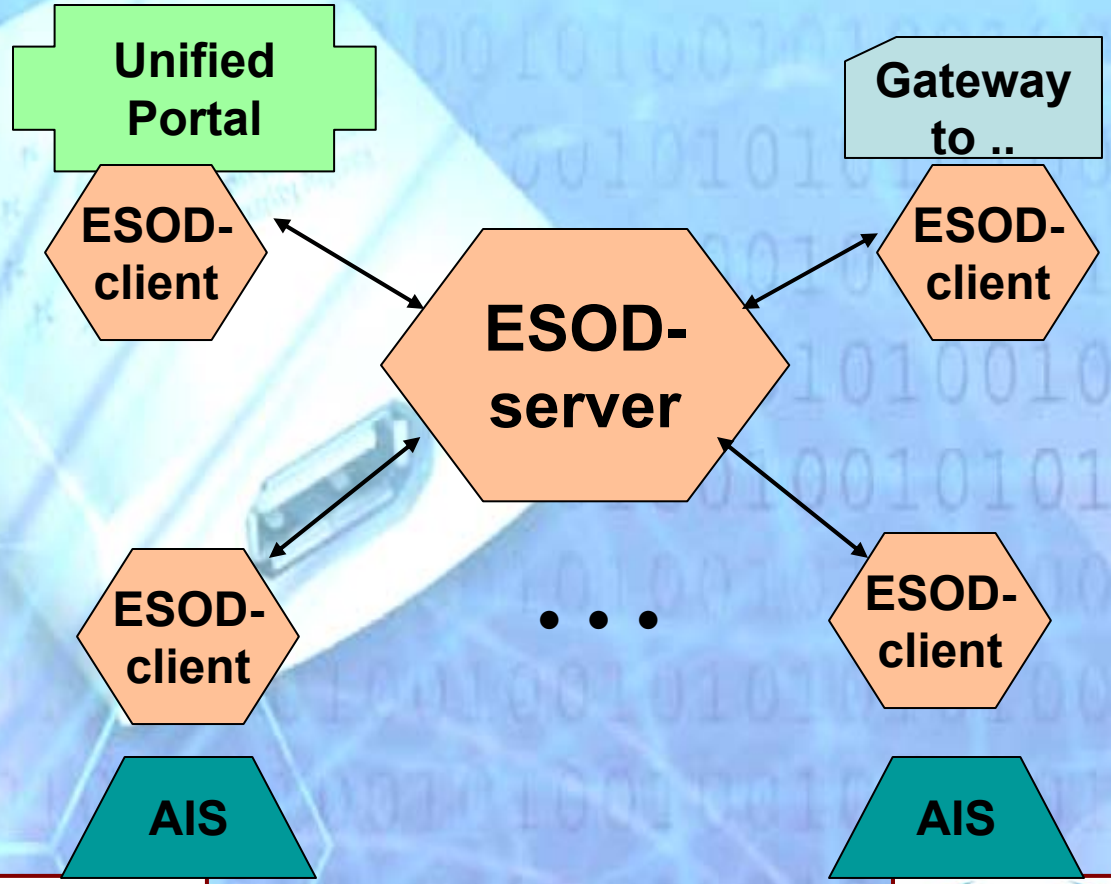
In accordance with the Regulation SAITC establishes Governmental CSIRT with assistance of ENISA and the Hungarian Gov-Cert.

This unit will play a part of a National CERT.

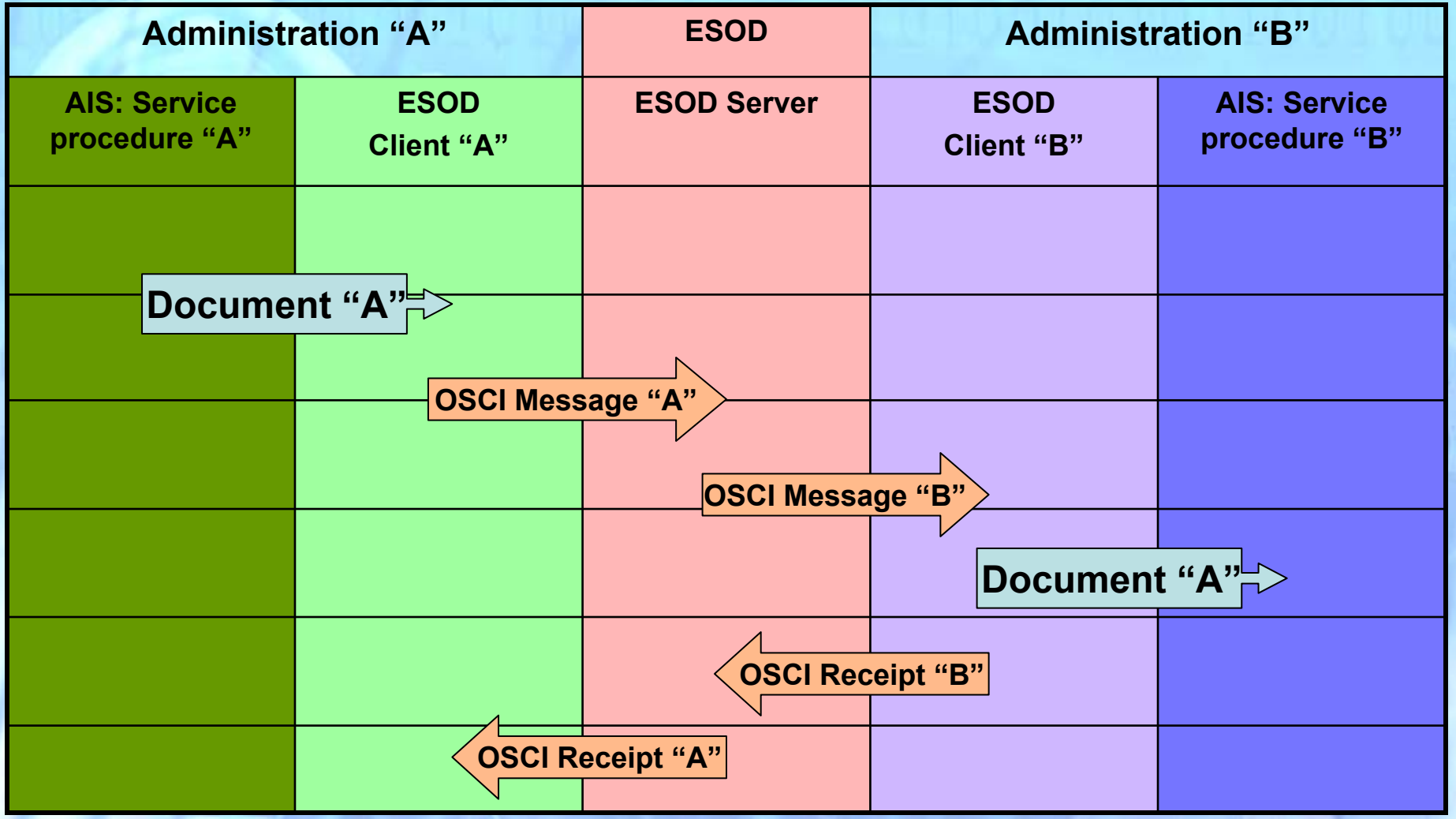


Unified environment for secure exchange of electronic documents (ESOD)

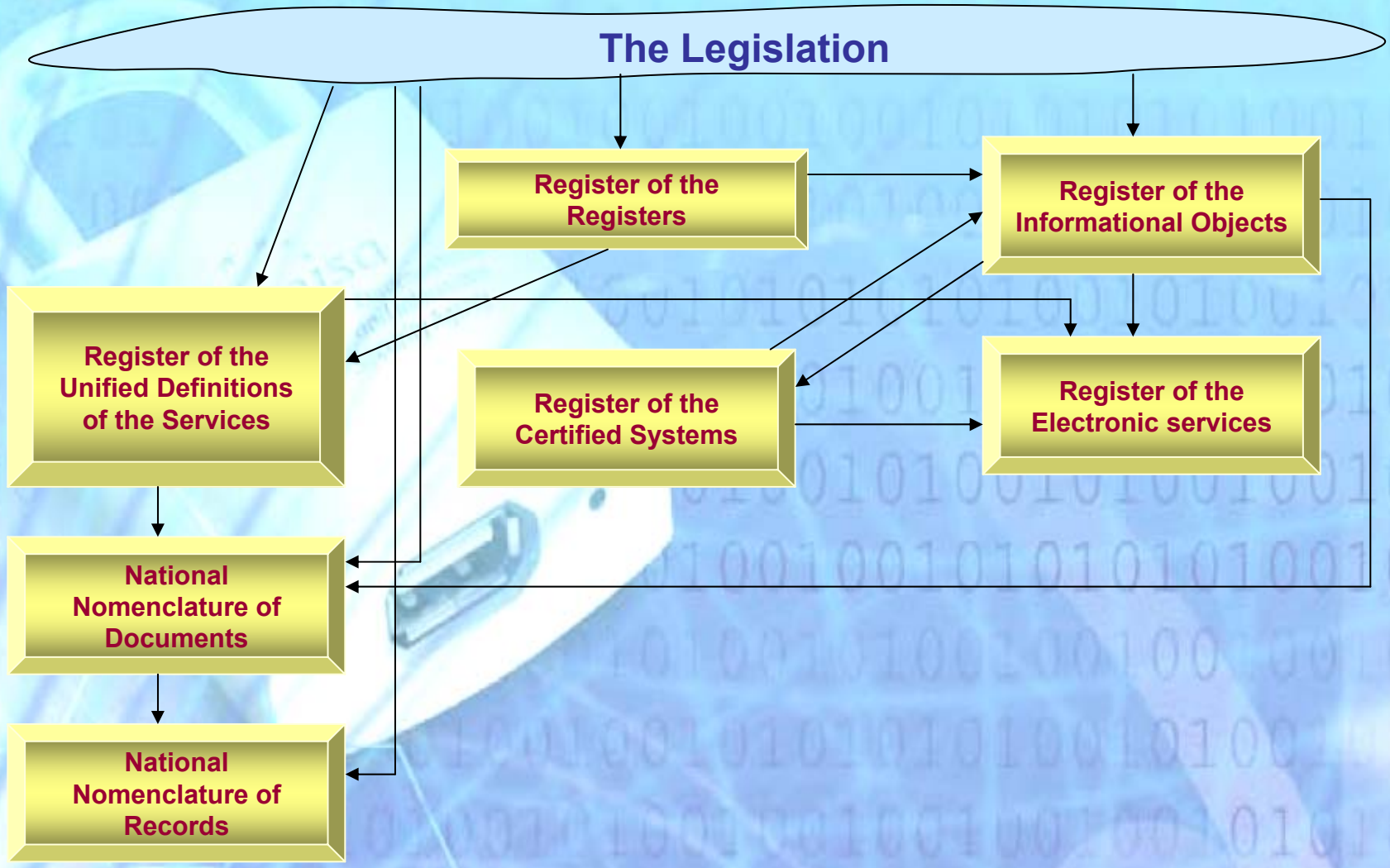
ESOD is manageable environment for standardized secure exchange of certified e-Documents between registered persons.



The exchange of documents through ESOD



The National Administrative Data Model



Specific Certification of Administrative Information Systems

The Chairman of SAITC:
- accredits assessors;
- maintains a publicly accessible register of accredited persons;
- empowers officials to monitor accredited assessors.

The accredited assessor checks up the system to verify compliance with the requirements of the Regulation and on positive issues relevant certificate.

Certification of Administrative Bodies

This is a certification procedure of the "system for information security management" of administrative body in a way of the international standard ISO 27001:2005.

The procedure includes:

- assets management;
- risk assessment and treatment;
- access control;
- communications and operations management;
- protection against malicious code;
- monitoring and incident management;
- physical and environmenta security;
- human resources security.

Conclusions

The Electronic Governance act and the six subsidiary regulations as a whole create consistent and functionally complete environment of requirements for network and information security of administrative information systems.

These requirements are aimed primarily at ensuring the smooth exchange of so called internal electronic administrative services between administrations and the opportunity that the electronic administrative services provided by each body can be included in the value-added chains.