Workshop on Data Access to Micro-Data (WDA)

Nuernberg, August 20-21

An Overview of Secure and Authenticated Remote Access to Central Sites

Dr Milan Marković
Banca Intesa ad Beograd, Serbia
milan.markovic@bancaintesabeograd.com

Content

- Introduction
- Potential Vulnerabilities in Modern Computer Networks
- PKI (Public Key Infrastructure) Systems
- Multilayered Security Infrastructures
- User Authentication Procedures
- Smart Cards and Hardware Security Modules (HSM)
- Security of Central Organization Sites
- M-government and authentication – FP6 project SWEB as an example
- Conclusions

Introduction

- This paper is devoted to the emerging topic in domain of modern e-business systems – a computer network security based on Public Key Infrastructure (PKI) systems and, particularly, to the user strong authentication procedures for remote access to the central sites.
- First, we consider possible vulnerabilities of the TCP/IP computer networks and possible techniques to eliminate them.
- We signify that only a multilayered security infrastructure could cope with possible attacks to the computer network systems.
- We evaluate security mechanisms on application, transport and network layers of ISO/OSI reference model and give examples of the today most popular security protocols applied in each of the mentioned layers.

Introduction

- We recommend secure computer network systems that consist of combined security mechanisms on three different ISO/OSI reference model layers:
  - network IP layer security providing bulk security mechanisms on network level between network nodes,
  - transport layer security based on establishment of a cryptographic tunnel between network nodes and strong node authentication procedure and
  - application layer security based on strong user authentication, digital signature, confidentiality protection, digital certificates and hardware tokens.
- User strong authentication procedures based on digital certificates and PKI systems are especially emphasized.

Introduction

- Organizations must create secure architecture to protect the privacy of user data.
- Such data could be:
  - Internal users (corporates with internal computer networks)
  - External users (external users – private and legal persons, customers, third parties – for organizations as banks, telecom operators, etc.)
  - E-government systems (citizens, business, government itself – G2C, G2B, G2G systems).

Potential Vulnerabilities in Modern Computer Network Systems

- Identity theft, phishing
- Eavesdropping
- Data modification
- Identity spoofing (IP address spoofing)
- Password-based attacks
- Denial-of-service attack
- Man-in-the-middle attack
- Compromised-key attack
- Sniffer attack
- Application-layer attack

Possible ways to prevent attacks

- **Encryption** – confidentiality protection of data and passwords,
- **Digital signature technology** – providing authenticity, integrity protection and nonrepudiation,
- **Strong authentication procedure** – secure authentication between communication parties,
- **Using of strong keys and frequent key changing** – prevent the cryptoanalysis,

Possible ways of prevent attacks

- **Network address translation (protection)** – protection from denial-of-service attacks,
- **Using of PKI digital certificates** – as unique electronic ID of communication parties,
- **Smart card usage** – for generating keys, secure storing keys and for generating of digital signatures,
- **Appropriate antivirus, antispam, antiphishing protection,**
- **Intrusion prevention systems**.

Security technologies

- The main cryptographic aspects of the modern computer TCP/IP networks:
  - Digital signature technology based on asymmetrical cryptographic systems
  - Confidentiality protection based on symmetrical cryptographic algorithms
  - PKI – Public Key Infrastructure

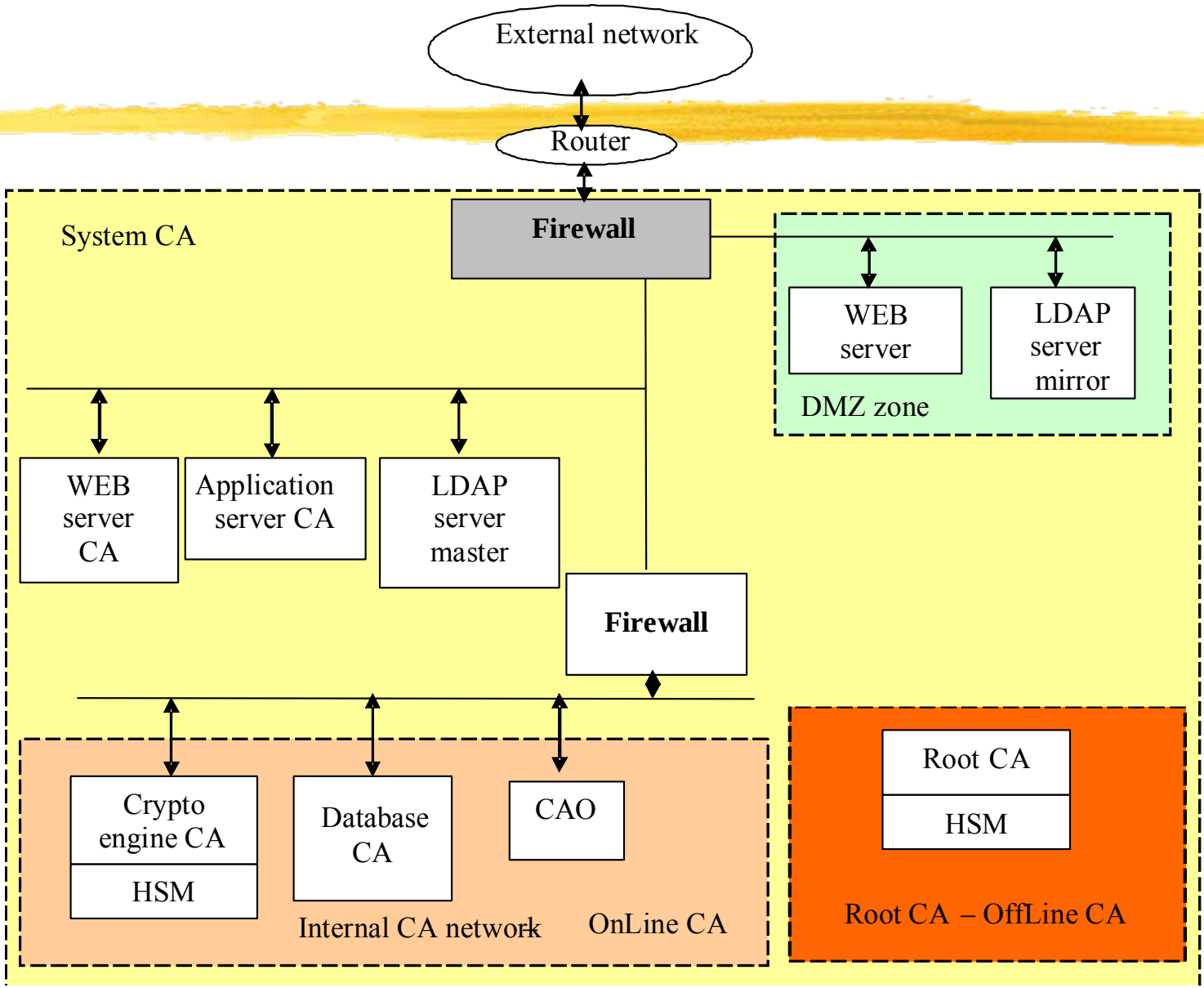
PKI Systems

- In the sense of ITU-T X.509 standard, the PKI system is defined as the set of hardware, software, roles and procedures needed to create, manage, store, distribute and revoke certificates based on public-key cryptography.
- PKI system provides a reliable organizational, logical and technical security environment for realization of the four main security functions of the e-business systems:
  - authenticity,
  - data integrity protection,
  - non-repudiation and
  - data confidentiality protection.
- PKI systems are based on digital certificates as unique cryptographic based electronic IDs of relying parties in some computer networks.

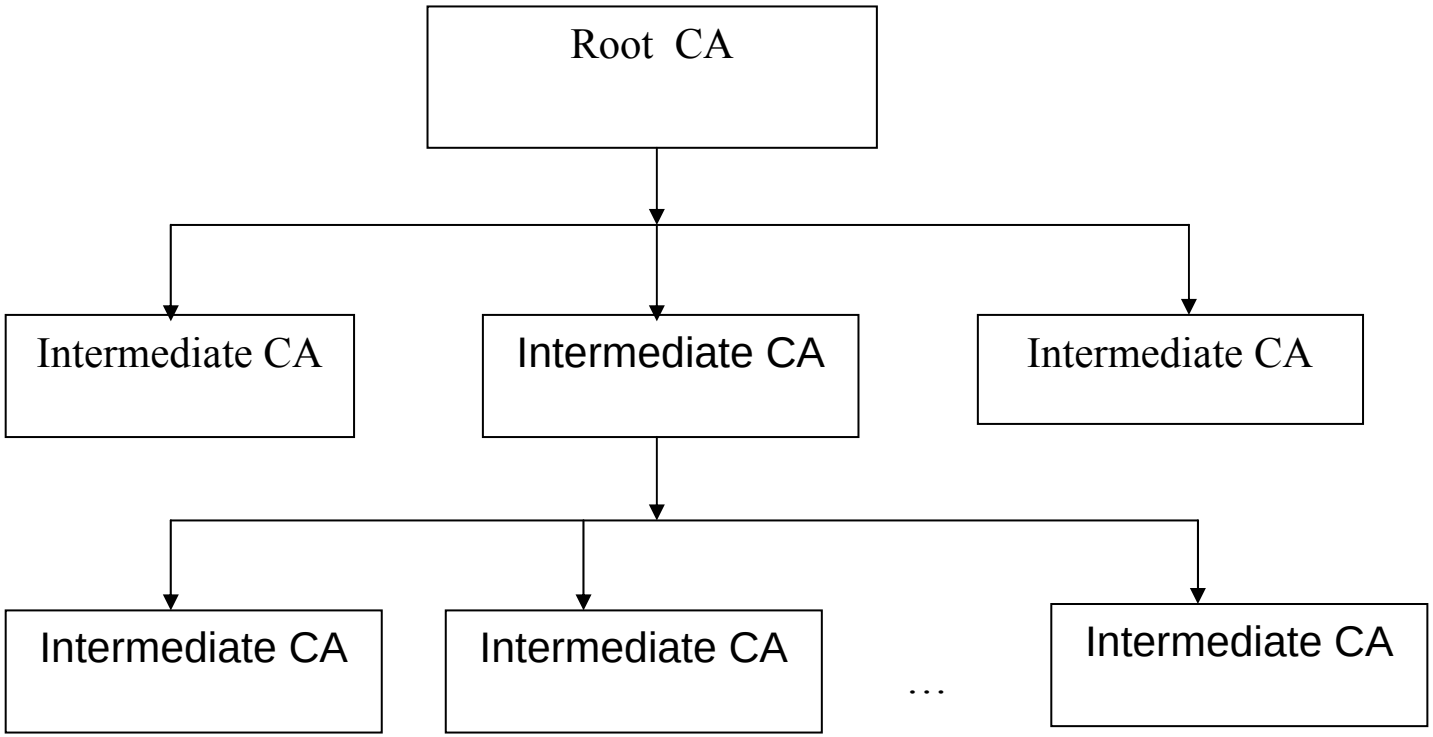
PKI Systems

- PKI system consists of the following components:
  - Certification Authority (CA) – responsible for issuing, renewing and revoking certificates and CRLs,
  - Registration Authorities (RAs) – responsible for acquiring certificate requests and checking the identity of the certificate holders,
  - Systems for certificate distribution – responsible for delivering the certificates to their holders,
  - Certificate holders (subjects) – people, machines or software agents that have been issued with certificates,
  - CP, CPS, user agreements and other basic CA documents,
  - Systems for publication Certificate Revocation Lists (CRLs),
  - PKI applications (secure WEB transactions, secure E-mail, secure FTP, VPN, secure Internet payment, secure document management system – secure digital archives, logical access control system, etc.)

Generic PKI System - architecture



Generic PKI System - hierarchy



Multilayered Security Infrastructure

- Key security features that should be included in modern computer networks are:
  - user and data authentication,
  - data integrity,
  - non-repudiation, and
  - confidentiality.

Multilayered Security Infrastructure

- This means that in secure computer network systems, the following features must be realized:
  - strong user authentication,
  - integrity of data transferred either via wired or wireless IP networks and
  - the non-repudiation function.
- These features are to be implemented by using strong user authentication procedures and digital signature technology based on asymmetrical cryptographic algorithms.
- Besides, the confidentiality and privacy protection of transferred data must be preserved during whole transmission and they are to be done by using symmetrical cryptographic algorithms.

Multilayered Security Infrastructure

- Modern computer networks security systems consist of security mechanisms on three different ISO/OSI reference model layers:
  - Network IP level security providing bulk security mechanisms on network level between network nodes – protection from the external network attacks.
  - Transport level security based on establishment of a cryptographic tunnel (symmetric cryptography) between network nodes and strong node authentication procedure,
  - Application level security (end-to-end security) based on the strong user authentication, digital signature, confidentiality protection, digital certificates and hardware tokens (e.g. smart cards),

Network level security mechanisms

- Network level security mechanisms include security mechanisms implemented in communication devices, firewalls, operating system security mechanisms, etc.
- These methods represent the basis for realization of Virtual Private Networks (VPN). Security protection is achieved by encrypting the complete IP traffic (link encryption) between two network nodes.
- The most popular network layer security protocols are: IPSec (AH, ESP, IKE), packet filtering and network tunnelling protocols, and the widest used is IPSec.
- Like transport level security protocols, IPSec consists also of network node authentication based on asymmetrical cryptographic algorithms and link encryption based on symmetrical algorithms.

IPSec

- IPSec framework consists of three main components:
  - Authentication Header (AH),
  - Encapsulating Security Payload (ESP), and
  - Internet Key Exchange (IKE).
- IPsec adds integrity checking, authentication, encryption and replay protection to IP packets.

VPN implementations

- Today's popular VPN implementation methods:
  - GRE
  - IPsec
  - PPTP
  - L2TP
  - MPLS
  - SSL VPN

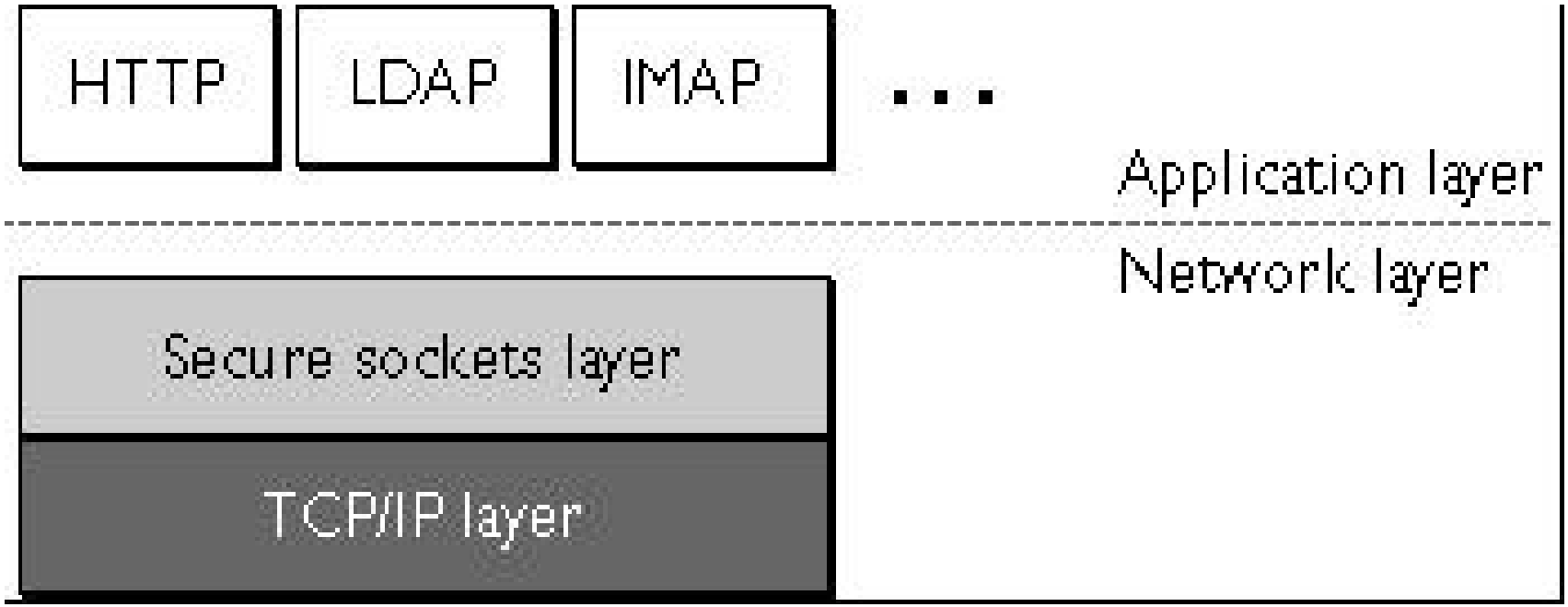
Transport level security mechanisms

- Security mechanisms on transport level generally include confidentiality protection of transmitted data based on symmetrical cryptographic algorithms.
- These systems are mostly based on establishing the cryptographic tunnel between two network nodes on transport level. The establishment of the tunnel is preceded by strong authentication procedures.

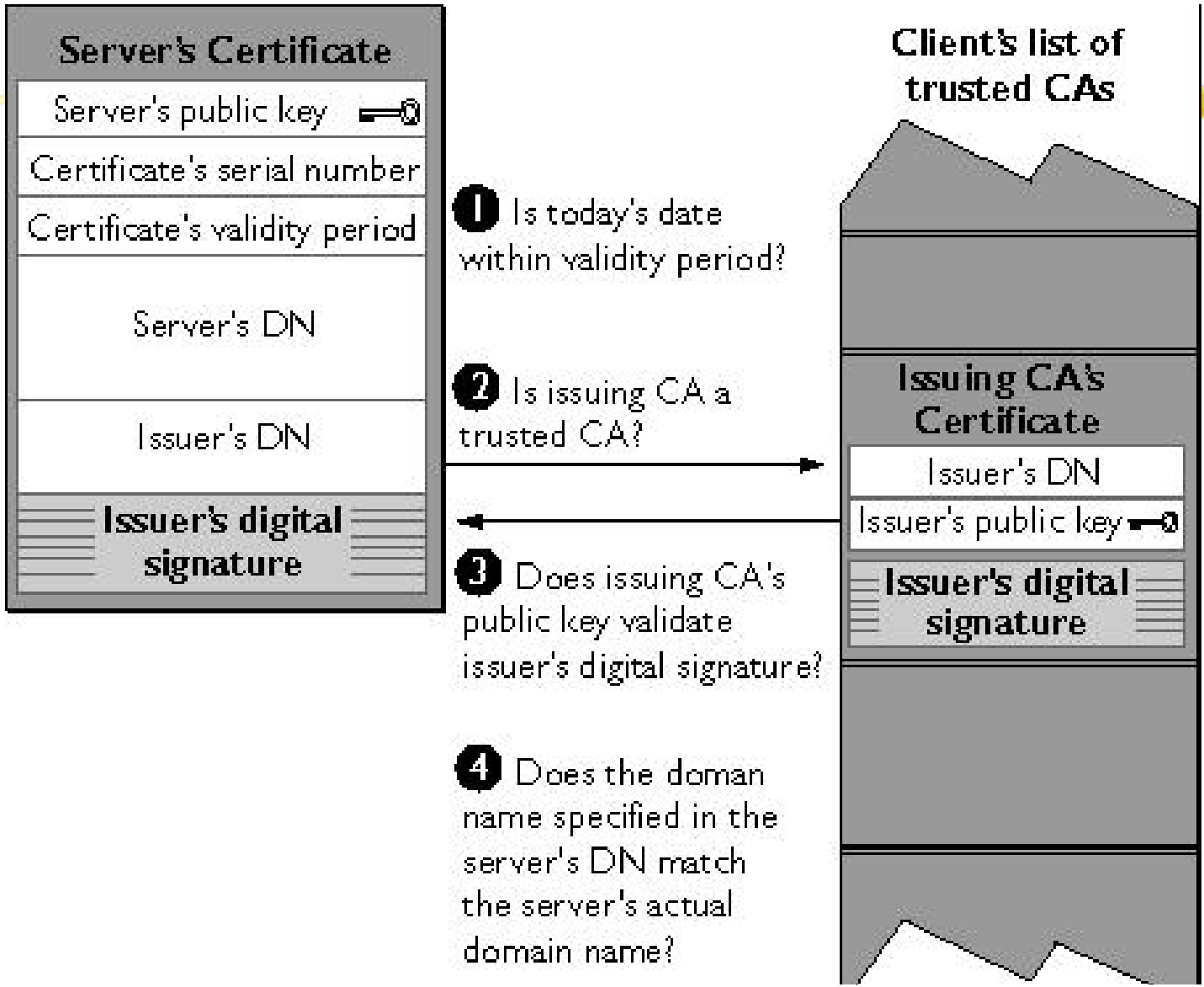
Transport level security mechanisms

- In this sense, the systems are based both on symmetrical algorithms for realization of cryptographic tunnel and a bilateral challenge-response authentication procedure based on asymmetrical algorithms and PKI digital certificates for authentication of the nodes and for establishing the symmetrical session key for this tunnel session.
- The transport level security system is mostly used for communication protection between client with Internet browser programs (Internet Explorer, Netscape Navigator, etc.) and WEB server, and the most popular protocols are: SOCKS (used earlier), SSL/TLS and WTLS. Between them, the most popular is SSL (Secure Sockets Layer) protocol, which is used for protection between client browser program and WEB server. Furthermore, SSL is the most popular and the far widest used security protocol today.

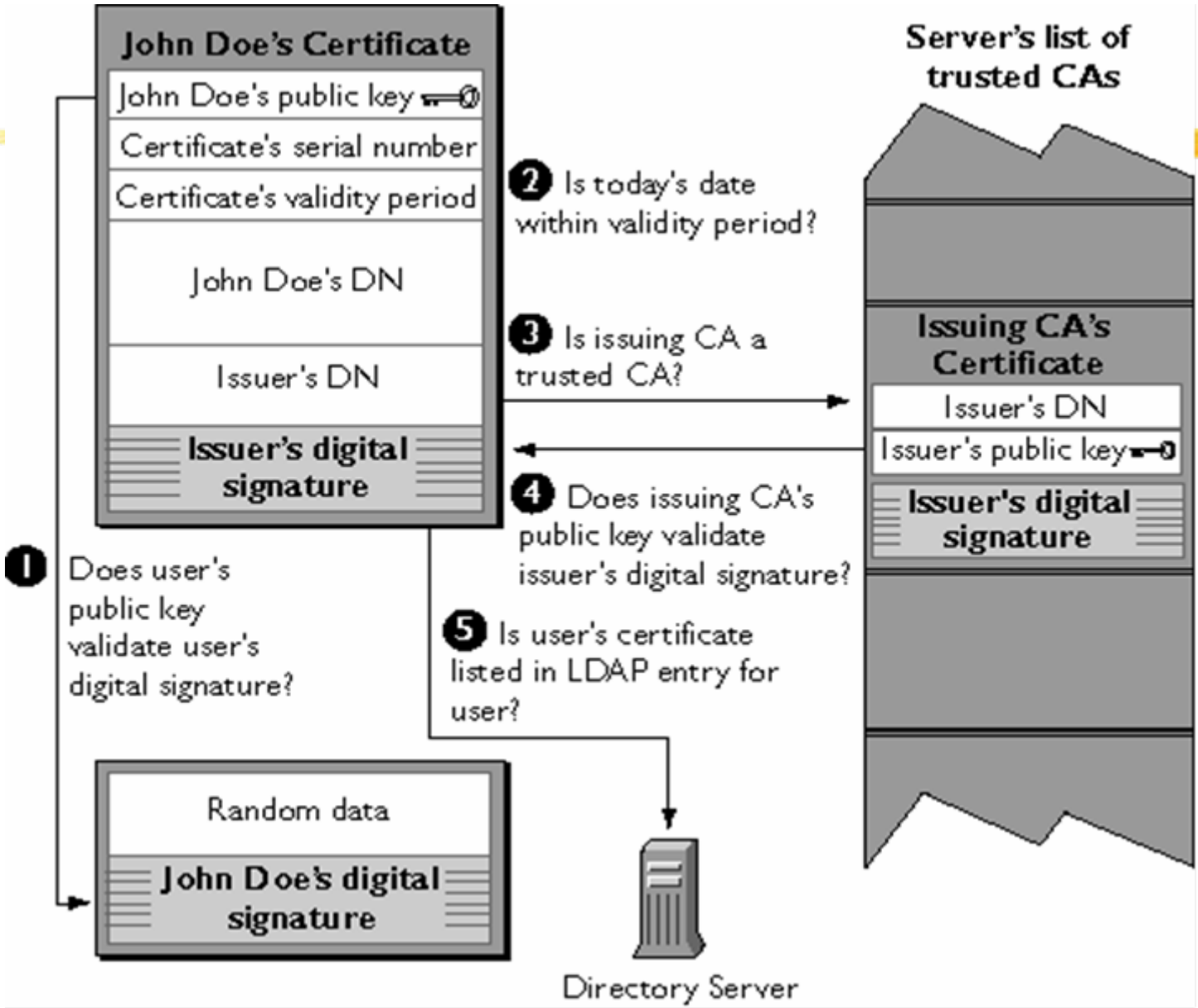
SSL protocol



Server authentication



Client authentication



Application level security mechanisms

- Application level security mechanisms are based on asymmetrical and symmetrical cryptographic systems, which realize the following functions:
  - Authenticity of the relying parties (asymmetrical systems),
  - Integrity protection of transmitted data (asymmetrical systems),
  - Non-repudiation (asymmetrical systems),
  - Confidentiality protection on application level (symmetrical systems).
- The most popular protocols in domain of application level security are: S/MIME, PGP, Kerberos, proxy servers on application level, SET, crypto APIs for client-server applications, etc.

Application level security mechanisms

- Most of these protocols are based on PKI X.509 digital certificates, digital signature technology based on asymmetrical algorithms (e.g. RSA, DSA, ECDSA) and hash functions (MD5, RIPEND160, SHA-1, SHA-224, -256, -384, -512) and confidentiality protection based on symmetrical algorithms (e.g. DES, 3DES, IDEA, AES, RC4, etc.).
- Most of the modern application level security protocols, such as: S/MIME and crypto APIs in client-server applications are based on digital signature and digital envelope technology.

User authentication

- Security systems on application level consist also of the user authentication procedure which could be one, two or three-component authentication procedure.
- There are several types of user authentication procedures that could be based on the following components:
  - Username/Password – PIN code – something that user know,
  - hardware token – something that user has, and
  - biometric characteristic (e.g. fingerprint) – something that user is.

User authentication

- Regarding the above components there are several types of authentication procedures which combine some of them, such as:
  - Username/password based authentication – weak authentication,
  - Username + dynamic password (one-time password) obtained by appropriate hardware token – stronger than previous one but not in the class of strong user authentication procedures,
  - Username + dynamic password obtained by appropriate hardware token + challenge-response procedure – strong user authentication procedure,

User authentication

- Username/password or PIN code + PKI smart card + bilateral challenge response procedure based on PKI X.509 digital certificate and asymmetrical cryptographic techniques – strong user authentication procedure (stronger than the previous one),
- PKI smart card + biometric characteristic checking + bilateral challenge response procedure based on PKI X.509 digital certificate and asymmetrical cryptographic techniques – strong user authentication procedure.
- Username/password or PIN code + PKI smart card + biometric characteristic checking + bilateral challenge response procedure based on PKI X.509 digital certificate and asymmetrical cryptographic techniques – the strongest user authentication procedure.

Strong user authentication

- The class of strong user authentication procedures consists of the two or more component procedures and the use of the bilateral challenge-response procedure.

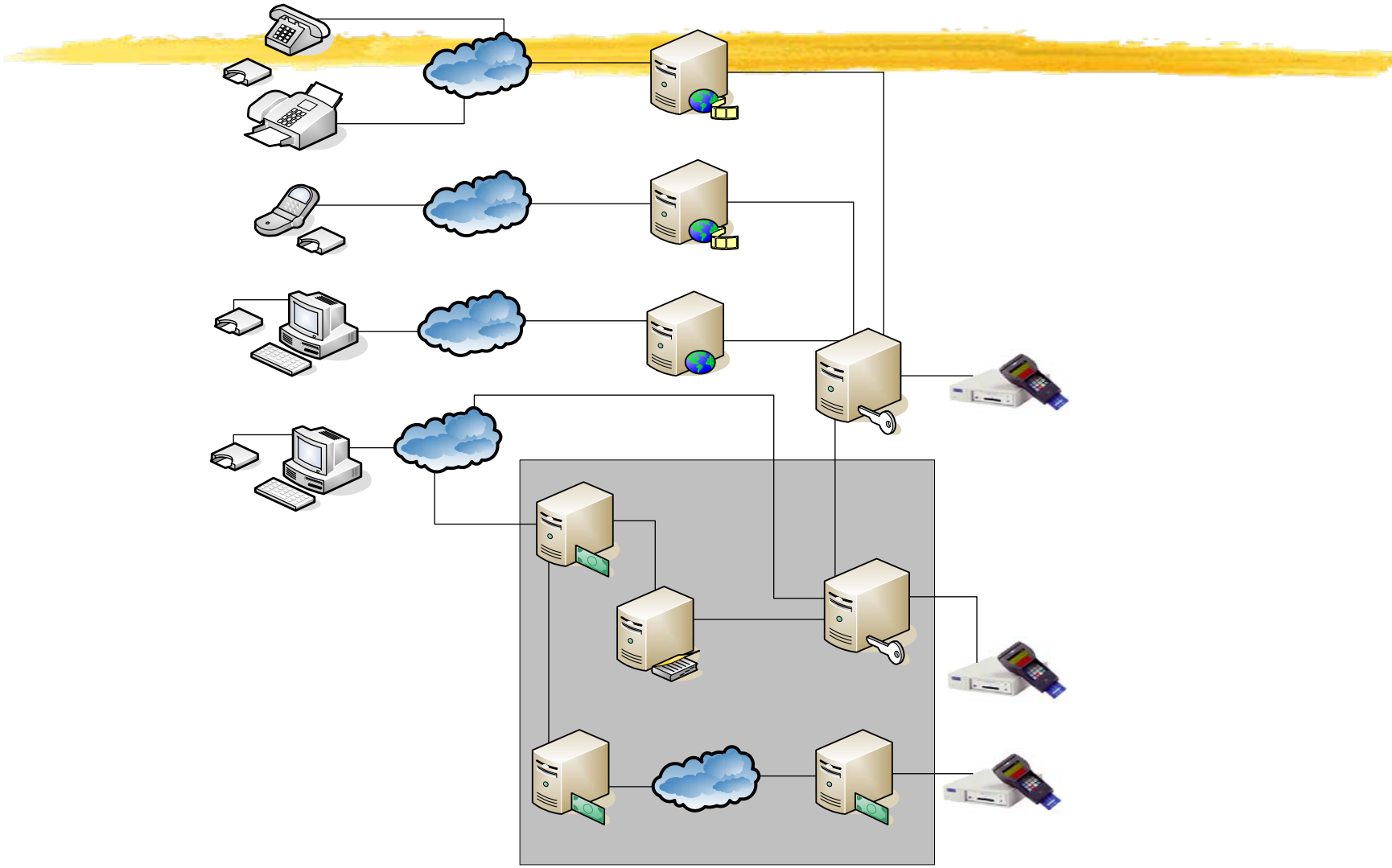
Strong user authentication as a part of logical security

- The information must be protected through appropriate protection measures so as to ensure that only the persons **identified, authenticated and authorized** may access the information.
  - **User Identification** – a process of recognition of a person through the verification of the existence of the user ID presented;
  - **User Authentication** - a process of verifying that the person identified is actually who he claims to be, by matching the credentials supplied with those registered;
  - **User Authorization** - a process of allowing a person the possibility of accessing the information requested, after the authentication has occurred.

Some examples of the strong (2F) user authentication systems

- SSL client authentication system based on user PKI X.509 digital certificate on the smart card
- SSL client authentication + username/password for authentication to the application
- SSL client authentication + username/dynamic password (OTP) for authentication to the application
- Proprietary authentication procedure on the application layer based on PKI X.509 digital certificate and smart cards for users

CAP as one example of One-Time Password systems



Smart Cards and HSMs

- Differences between software-only, hardware-only and combined software and hardware security systems.
- Therefore, ubiquitous smart cards and hardware security modules are considered.
- Hardware security modules (HSM) represent very important security aspect of the modern computer networks.
- Main purposes of the HSM are twofold: increasing the overall system security and accelerating cryptographic functions (asymmetric and symmetric algorithms, key generation, etc.).

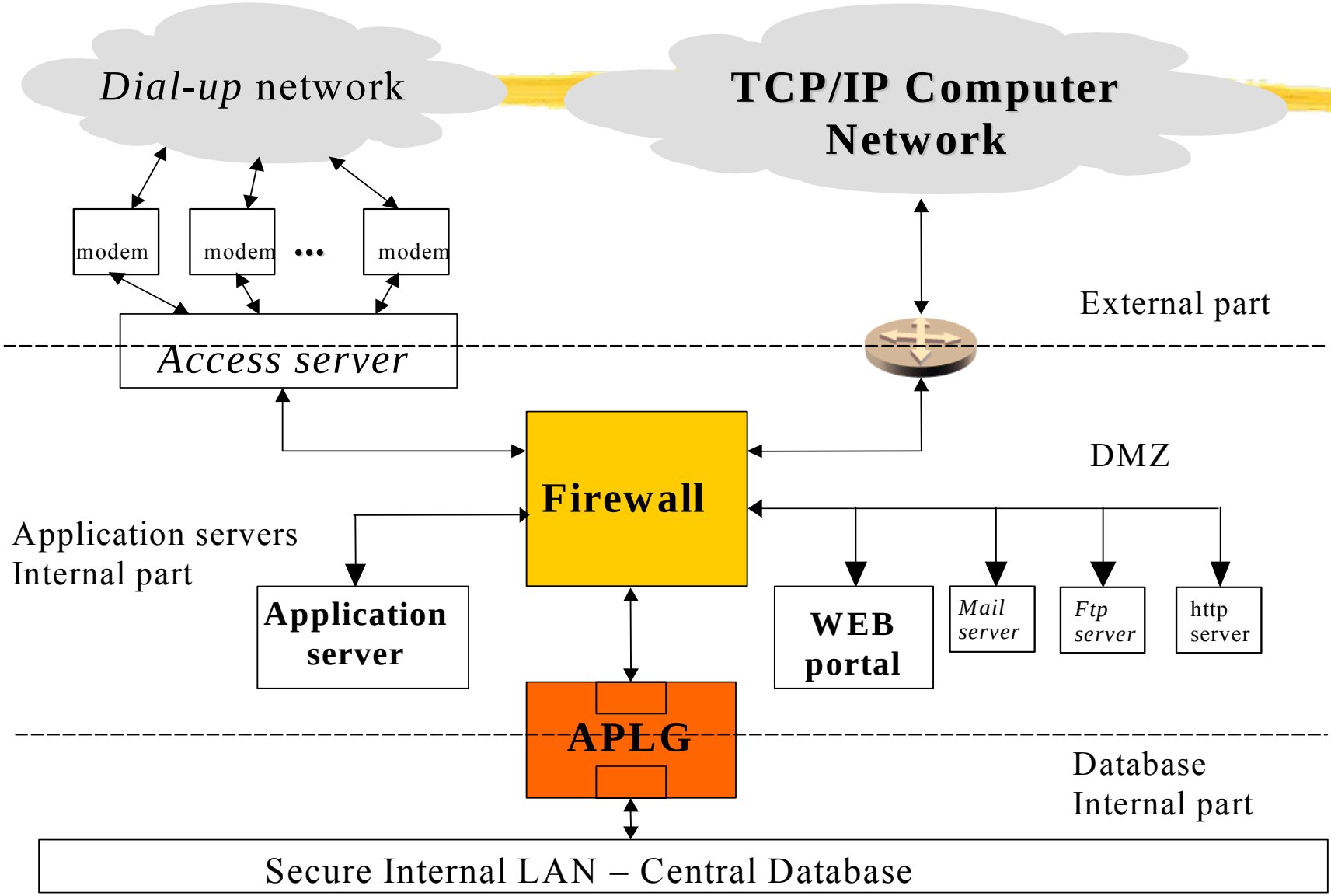
Smart Cards and HSMs

- HSMs are intended mainly for use in server applications and, optionally for client sides too in case of specialized information systems (government, military, police).
- For large individual usage, smart cards are more suitable as hardware security modules.
- However, for large usages, the best approach is in the combination of SW and smart card solutions for best performance.
- Namely, smart card increases security and SW increases the total processing speed. In this sense, the most suitable large-scale solution consists of: SW for bulk symmetric data encryption/decryption and smart card for digital envelop retrieval and digital signature generation.

Security Mechanisms for organizations

- Security mechanisms that are necessary to be implemented in the corporate information systems are:
  - strong user authentication procedure,
  - digital signature technology,
  - confidentiality protection of data in the system on the application, transport and network layers,
  - privacy protection of the user and customer data,
  - strong protection of the central database based on multiple firewall architecture, and
  - PKI systems, which issue X.509 digital certificates for all users of the system (internal and external users) - digital identities (IDs) for the users.

Generic model of the Central Secure Site



M-Government and authentication

- Starting with a fact that more citizens use mobile phones compared to computers.
- In Western Balkan countries this relation is even better on the side of mobile phones.
- Development of suitable e-services based on mobile phone application.

M-Government – Open Issues

- Performances of Mobile Terminals
- Available software tools and libraries
- Transmission Path performances
- Security
- User strong authentication

SWEB – FP6 project in domain of m-government

Secure, interoperable cross border m-services contributing towards a trustful European cooperation with the non-EU member Western Balkan countries

About SWEB

- SWEB is a 6th Framework Programme Project of the EU
- Priority: 2 - Information Society Technologies
- Instrument: Specific Targeted Research or Innovation Project (STREP)
- Strategic Objective: 2.6.5 - “International Cooperation for eGovernment and eParticipation” - Target Countries Western Balkans
- Contract Number 044979

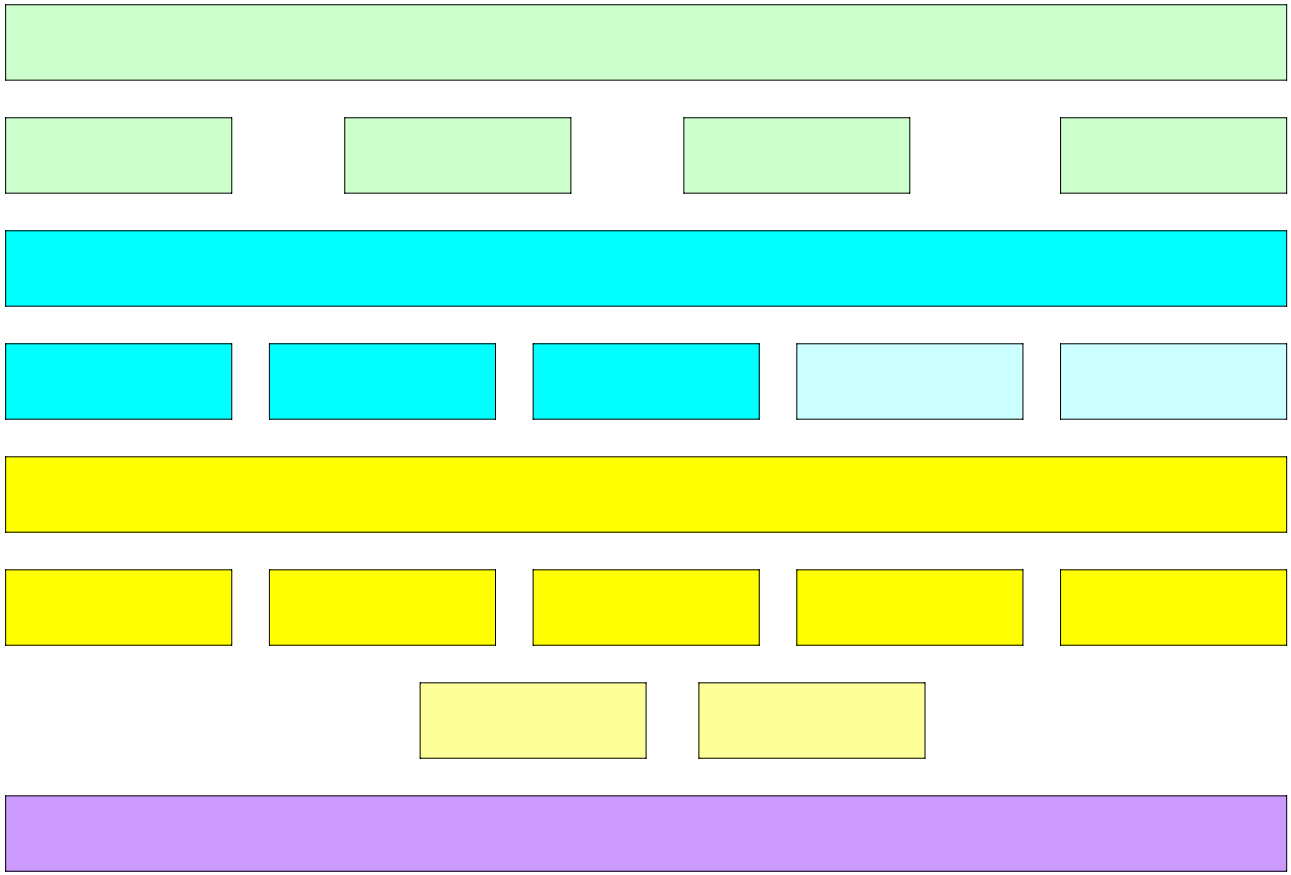
SWEB overall objective

- Development of a secure, interoperable, open, affordable platform upon which two secure cross border government services will be built:
  - *Residence Certification Service* as a specific example for a secure municipal document exchange service, in which a public organization and individual citizens can securely communicate e/m-municipal documents.
  - *Electronic/Mobile Invoicing*, which has a pivotal role in all the stages of handling Value Added Tax (VAT) for European Member States. Through e/m-invoicing, tax administrators will be able to implement new tools and procedures to carry out alternative controls.

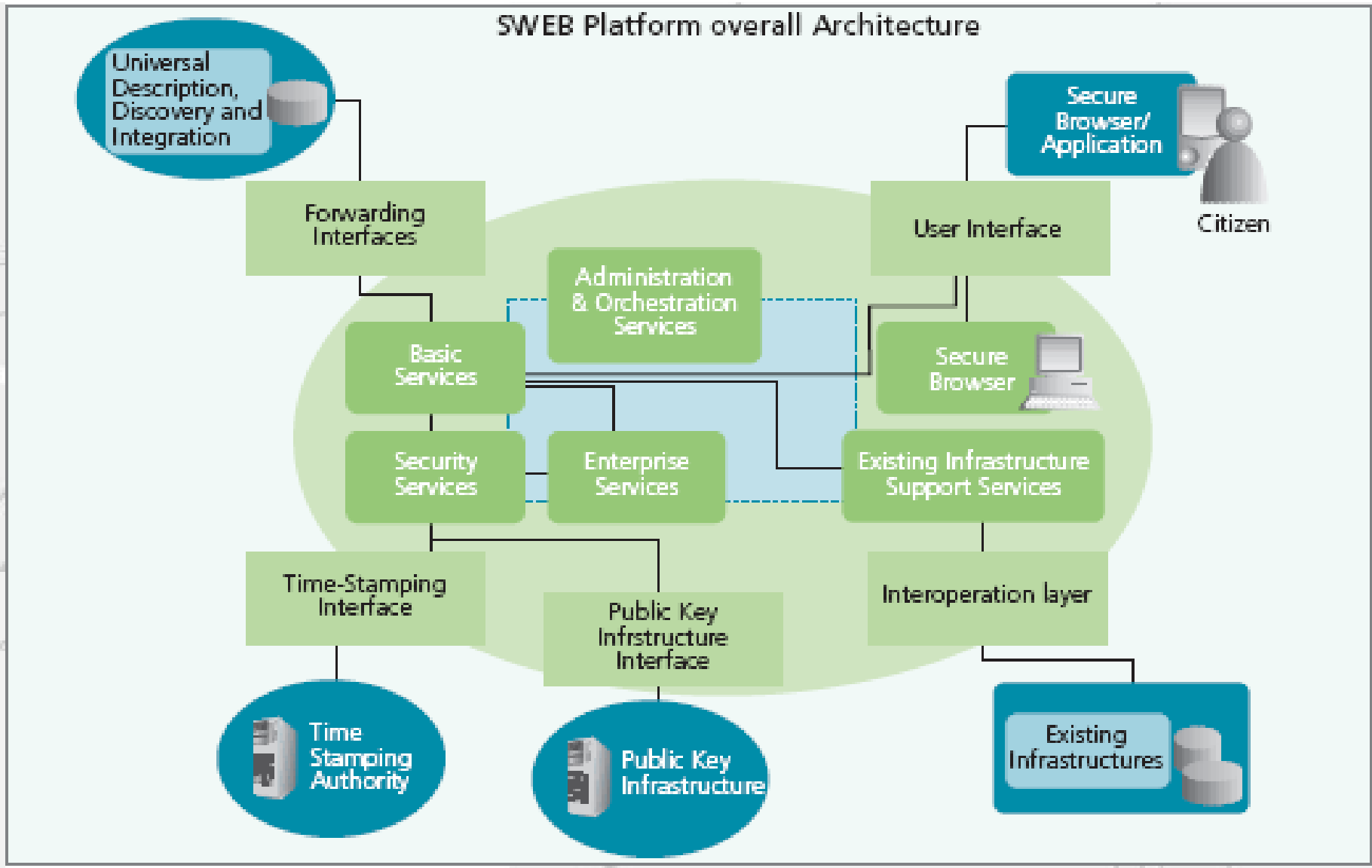
SWEB – Basic Data

- SWEB Start: 01.01.2007
- SWEB Duration: 27 months
- SWEB Partners: 12 (+ 4 Subcontractors)
  - EU: 4 Partners form Germany, Greece, Italy
  - NON-EU: 8 Partners from Serbia, FYROM, Albania

SWEB – Consortium



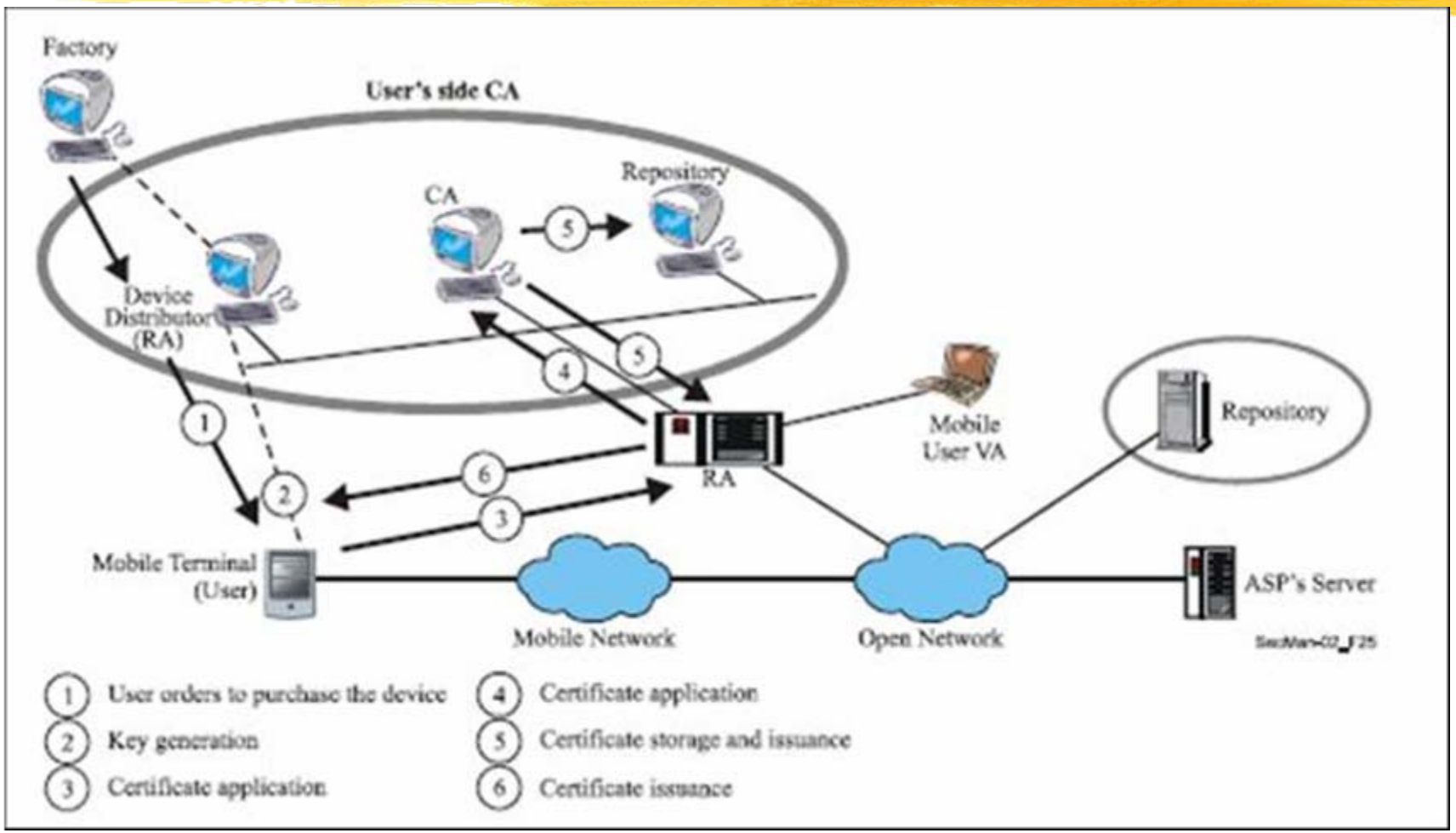
SWEB


SWEB Platform overall Architecture
Universal Description, Discovery and Integration
Secure Browser/ Application
Citizen
Forwarding Interfaces
User Interface
Administration & Orchestration Services
Basic Services
Secure Browser
Security Services
Enterprise Services
Existing Infrastructure Support Services
Time-Stamping Interface
Public Key Infrstructure Interface
Interoperation layer
Time Stamping Authority
Public Key Infrastructure
Existing Infrastructures

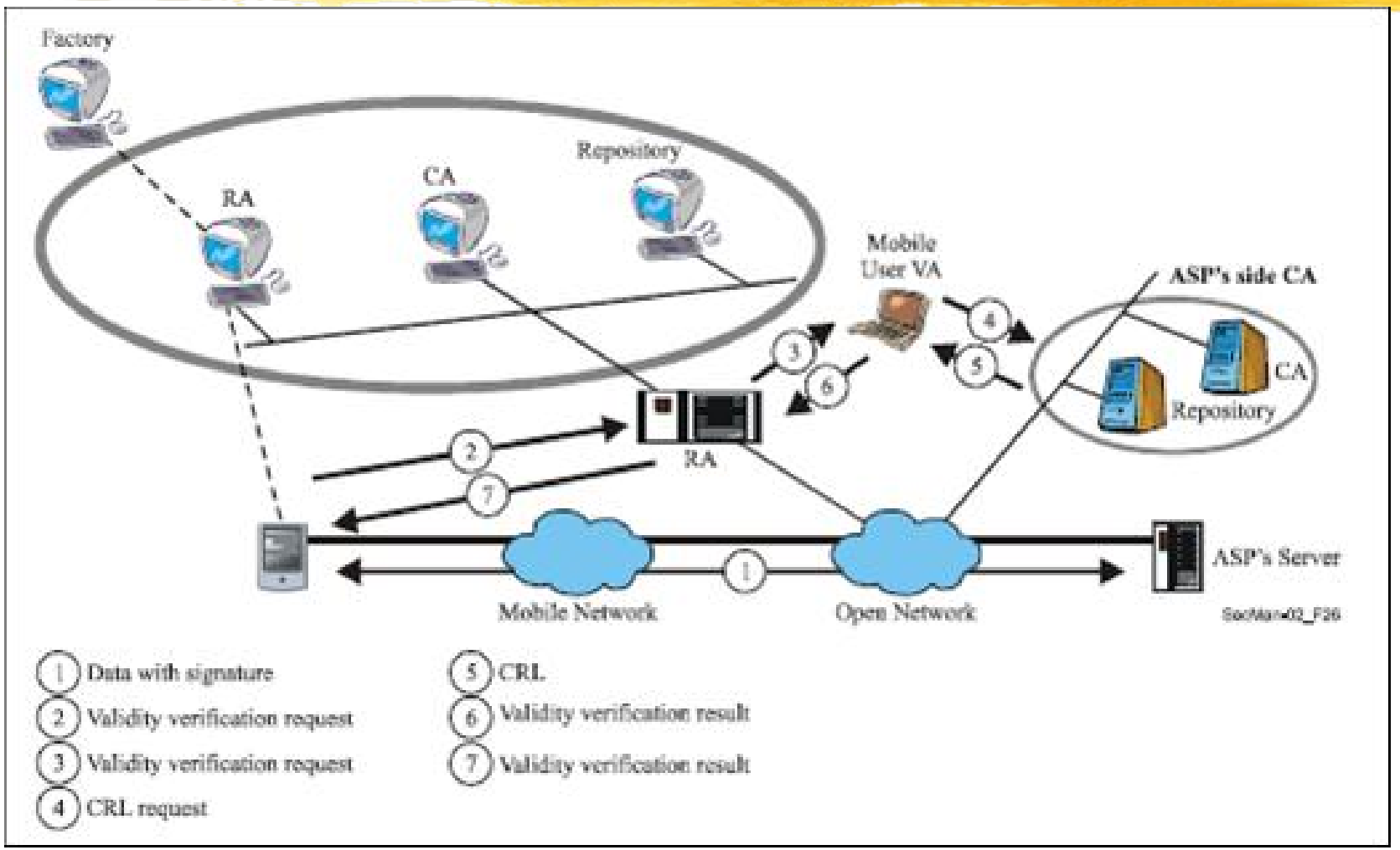
SWEB - tehnologies

- J2ME or .NET client applications
- WEB services and J2EE in the SWEB platform
- XML, SOAP
- Mobile PKI
- XKMS, OCSP, SAML, UDDI, WSPL
- XML security, WS-security
- SWEB Authentication and Authorization – digital certificates, SAML and XKMS.

M-government demands a mobile PKI system – user registration



M-government demands a mobile PKI system – certificate validation



Conclusion

- In this paper, data protection techniques, cryptographic protocols and PKI systems in the modern computer security systems are analyzed with special emphasis to the user strong authentication procedures.
- It is concluded that only multilayered security architecture including the user strong authentication procedure could cope with potential internal and external attacks to the modern computer networks.
- The most frequently used security mechanisms on the application, transport and network layers are analyzed.
- It is concluded that more than one layer should be covered by the appropriate security mechanisms in order to achieve high quality overall cryptography protection of the system.

Conclusion

- The analysis is done regarding security challenges and appropriate security mechanisms for coping with potential vulnerabilities.
- It is concluded that, between many specific conditions, in the particular e-business systems, security mechanisms should be distributed on the client side, communication side and central database side, and that, in each of the parts, appropriate security measures should be applied.
- Central points of the secure e-business systems are smart cards for end users that could be used for applying digital signature and digital envelope technology, as well as for 2F user strong authentication procedure, and the central PKI system.

Open questions

- Possibilities of merging computer network security techniques and SDC methods?
- Can we make a FP7 project proposal based on answers on the first question?
- Combining the statistical disclosure data analysis and computer network security evaluation of organizations (including banks, etc.)?
- Possible similar workshop in Belgrade?

THANKS FOR YOUR ATTENTION