Secure integration of distributed tools

- E-Colleg project solution

Adam Pawlak

Silesian University of Technology
Gliwice, Poland

MAPPER kick-off meeting

Mullsjö, Sweden
14-15.09.2005

Outline

- Towards a security framwork for VEs/VOs/CNs/CEEs
- Sources and potential threats
- Secure communication
    - Data confidentiality and integrity
- Authentication
- Authorization and access control
- Security management
- E-Colleg security framework
- Tool Registration and Management System
- Conclusions

Towards a security framwork for CEEs

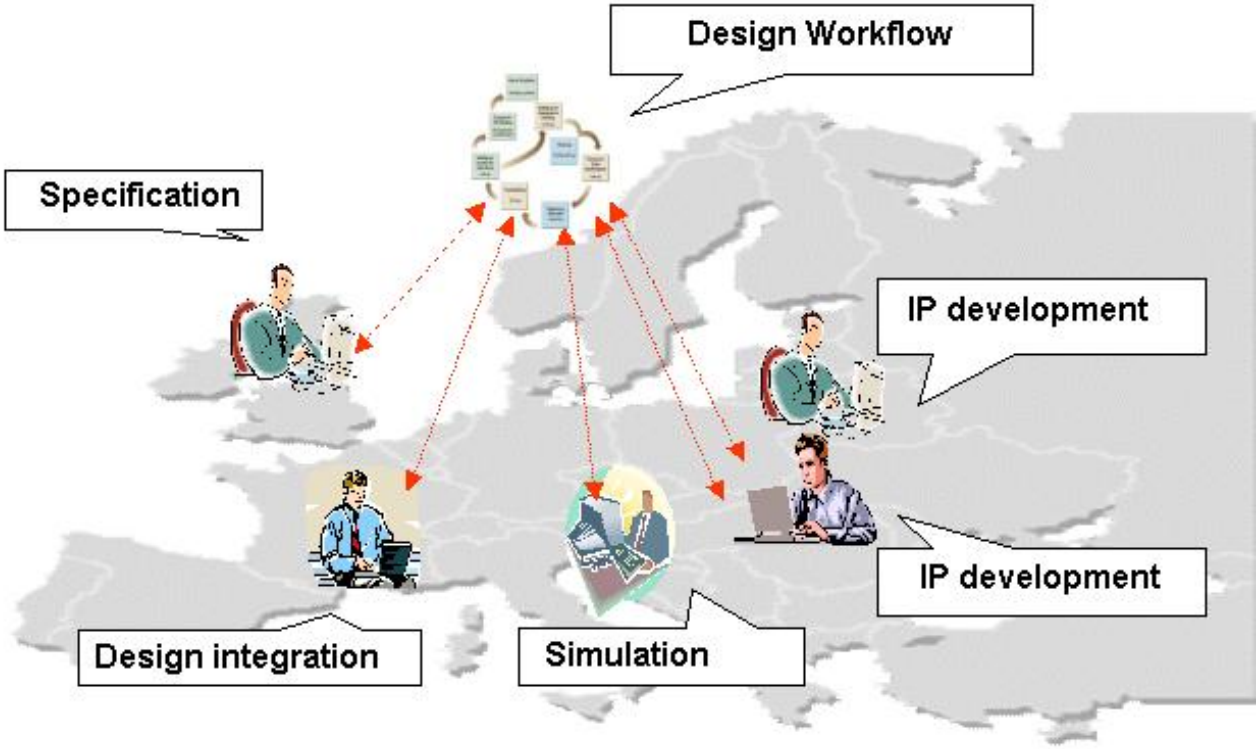
- **C**ollaborative **E**ngineering **E**nvironments require all „traditional” security precautions in computer systems and intra-organisations, *but additionally are needed*:
  - secure inter-organisational collaboration,
  - techniques for crossing borders of organisations (firewalls!),
  - secure communication.
- Two dimensions: human-engineers, tools

Why collaborative engineering in electronics

- *Time to market* is still the most significant factor for new product creation
- Thus, increase of design productivity is one of the major objectives within the SoC domain resolved by:
  - Structured design methodology with IP design reuse
  - Designing on higher levels of design abstraction
- Collaborative design is another approach allowing to increase design productivity of IP based SoC design with:
  - Easy and close collaboration of widely distributed engineers being experts in different domains and in different design flow phases
  - Controlled remote access to expensive design tools, etc.

Our motivation for collaborative design

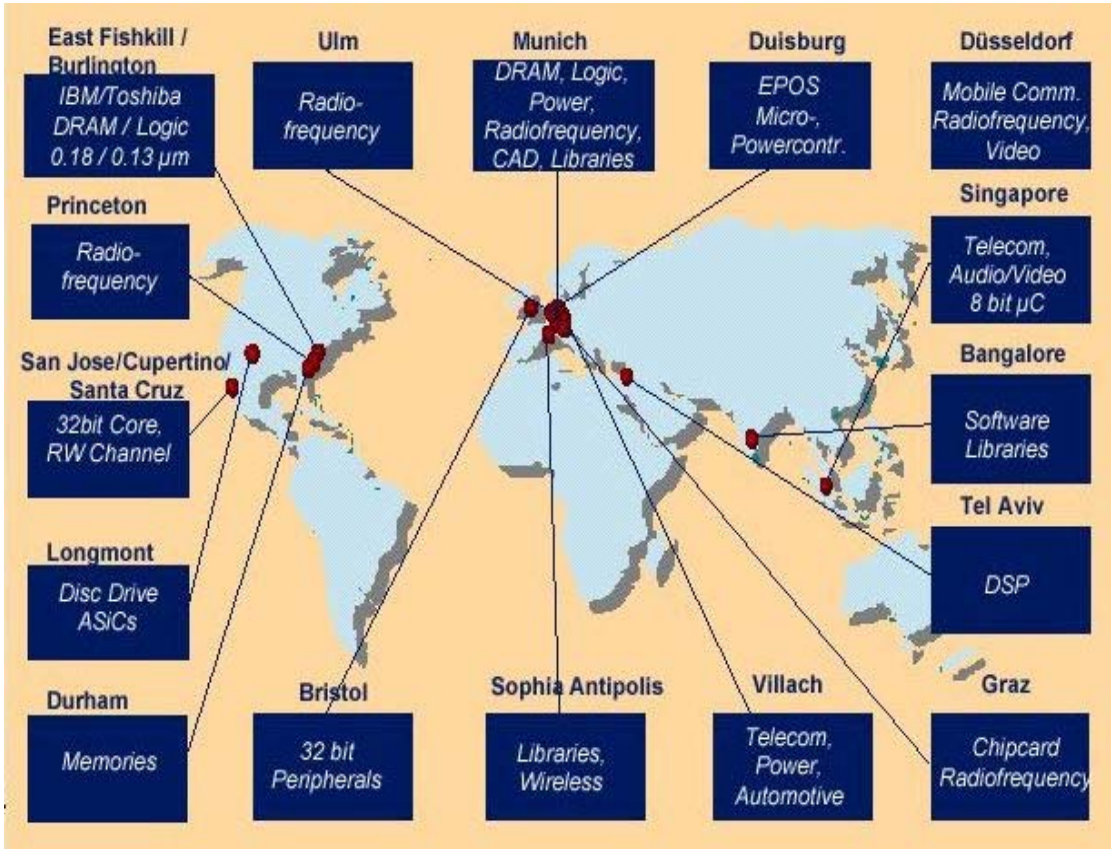
Integrating SMEs (from CEE countries) into complex design inter-organisational workflows



E-Colleg industrial partners motivation

the need for effiecient support to global distribution in engineering including outsourcing

Distributed collaboration over intranets is much better supported than collaboration between different organisations.



Courtesy: Dr. Matthias Bauer, Infineon Technologies

Selected Challenges in Collaborative Engineering

Establishment of an efficient collaborative engineering environment requires solving at least the following problems:

- Secure data transfer
- Collaboration with organisations protected behind firewalls
- Data format conformity, etc.
- Easy tool integration with standard support for:
  - Tool description
  - Task description
  - Workflow description
- Support for human actors – engineers collaborative actions
  - Advanced synchronous and asynchronous communication,

Threats to security of CNs 1/2

- Threats caused by an activity aiming at altering the present state of a system.
- Threats caused by activities aiming mainly at interception of information
- Threats resulting from various accidents and errors, as well as malfunction of the system

Threats to security of CNs 2/2

- A number of techniques are being employed these days to break the protection system:
  - masquerading, eavesdropping, modification of transmitted information, password hacking by force or by dictionary attack, analysis of traffic in the network, denial of service, social engineering, viruses, etc.
- Natural threats:
  - hardware damage, supply failure, fire, flood, etc.
- Different procedures of attacker:
  - Immediate effects (e.g. denial of service attack)
  - Results of attack unnoticed for a long time (eavesdropping, analysis of traffic in the network, etc.)

Secure communication, 1/2

- Data confidentiality -

  data transported by a network can be intercepted and read. Introduction of a mechanism, which will enable correct reading of contents only by entitled recipients is required.

- Data integrity -

  information can become consciously changed in the course of transport through a network by a third party. All attempts tamper with exchanged information should be signalled and changed message should be rejected by a receiver.

Secure communication, 2/2

- The most commonly used communication protocol TCP/IP does not have any built-in mechanisms securing the transmitted information. The task to secure confidentiality and integrity needs to shifted to upper layers of the ISO/OSI model
- Simultaneous securing of both confidentiality and integrity is not always demanded. In some cases securing integrity alone is sufficient.
- The most popular solutions securing communication:
  - Secure Socket Layer (SSL), Transport Security Layer (TSL)
  - Virtual Private Network (VPN) with IPSec Protocol
  - Encryption directly built-in into the application (e.g. PGP)

Authentication

- Authentication is a process in which the user identity, and the identity of a system element which is either an information source or an element demanding resource access, should be recognized and verified.
- Authentication is a base for other computer provided services such as authorization, access control and communication protection

- Various authenticating methods:
  - login/password, smart cards, PKI technology, digital signature, biometric systems, etc.

Authorization and access control

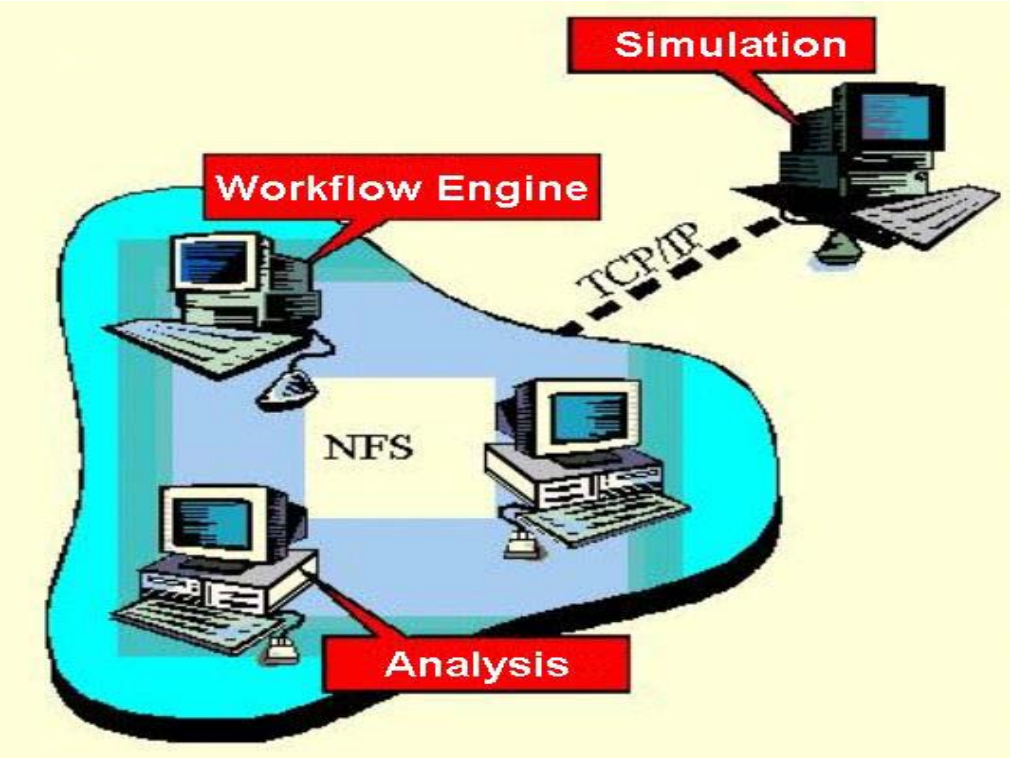
- Authorization - granted privileges for common resources are verified. A range of admitted privileges should be easily modifiable and enable realization of a project task. Flexible privileges management ought to be available.
- Access control - direct execution of granted privileges and a definitive decision about facilities of resources. Control should make impossible unauthorized access to resources.
- Selected solutions:
  - Access Control List (ACL) is commonly applied in authorization and access control process. The solution was taken from operating systems.
  - Authorization certificates are used in the new approach to authorization and access control.

Security management

- Security management objective and task is to reach and maintain the assumed security level of the information system.
- Security management is a continuous process in ever changing environment with new threats appearing and fast technology progress
- Three aspects: organizational, legal and technical.

E-Colleg Vision on security framework

E-Colleg has developed the technology that enables engineers located in remote sites to efficiently collaborate over the Internet.



R&D done on:

Advanced Collaborative Infrastructure (ACI) that will enable seamless Internet-based (multi-site and multi-platform) integration and management of tools and data.

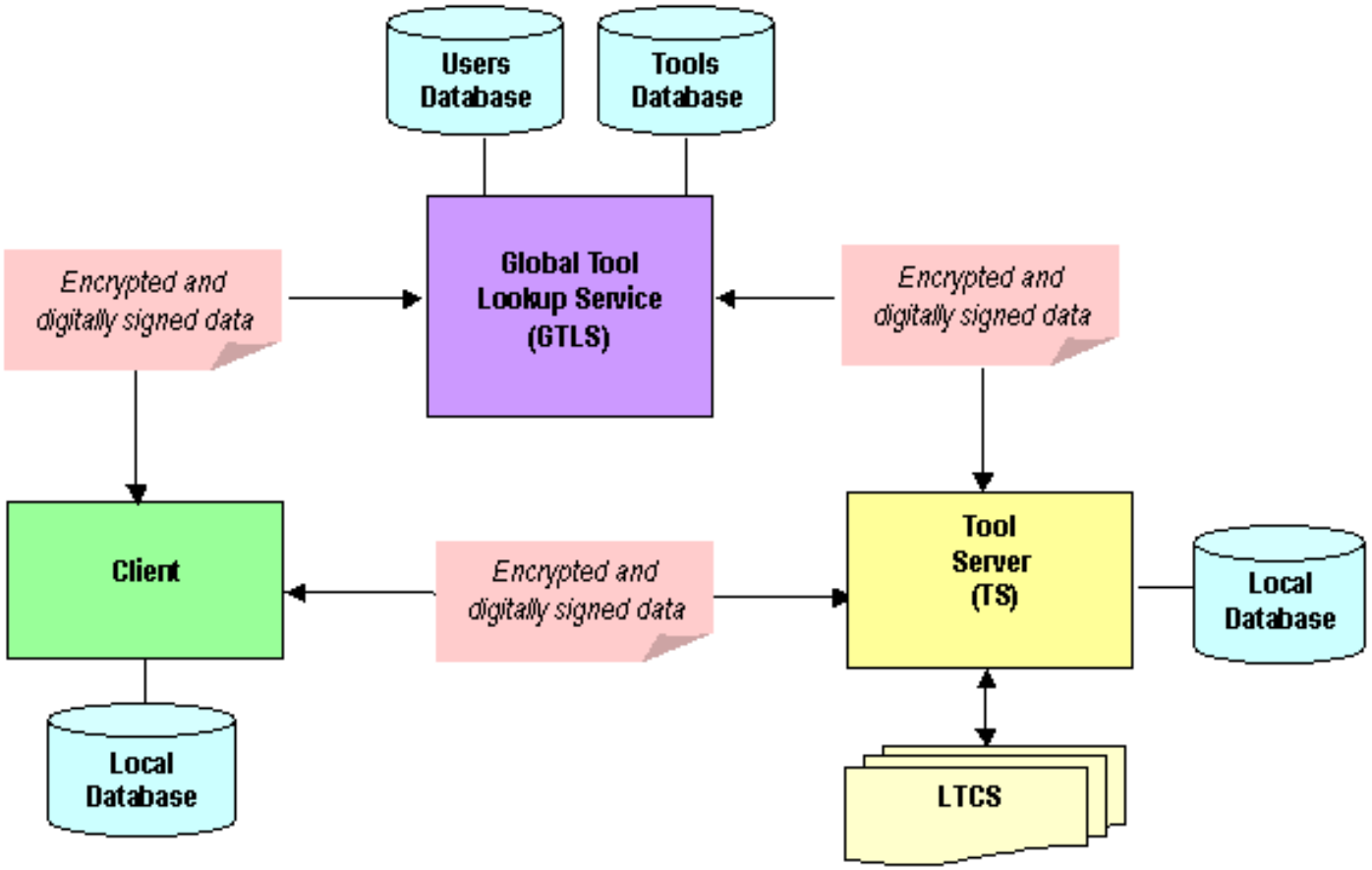
E-Colleg solution - TRMS

- TRMS – R&D by E-Colleg EU IST project provides means for enabling secure distributed engineering collaboration
- TRMS integrates Internet-wide distributed tools
- TRMS supports creation of CEEs
- Experiments are being conducted on TRMS deployment electronic engineering

Tool Registration and Management System

- Objectives:
  - Tool management
  - Search and invocation of distributed tools
  - Collaboration through firewalls
  - User management
  - Advanced and flexible definition of user's privileges
  - Tool Servers management
  - Creation of distributed workflows
  - Implementation of security mechanisms (encrypted data transfer, authentication with a digital signature, monitoring of users' activities)
  - Support for a proxy server

Architecture of TRMS

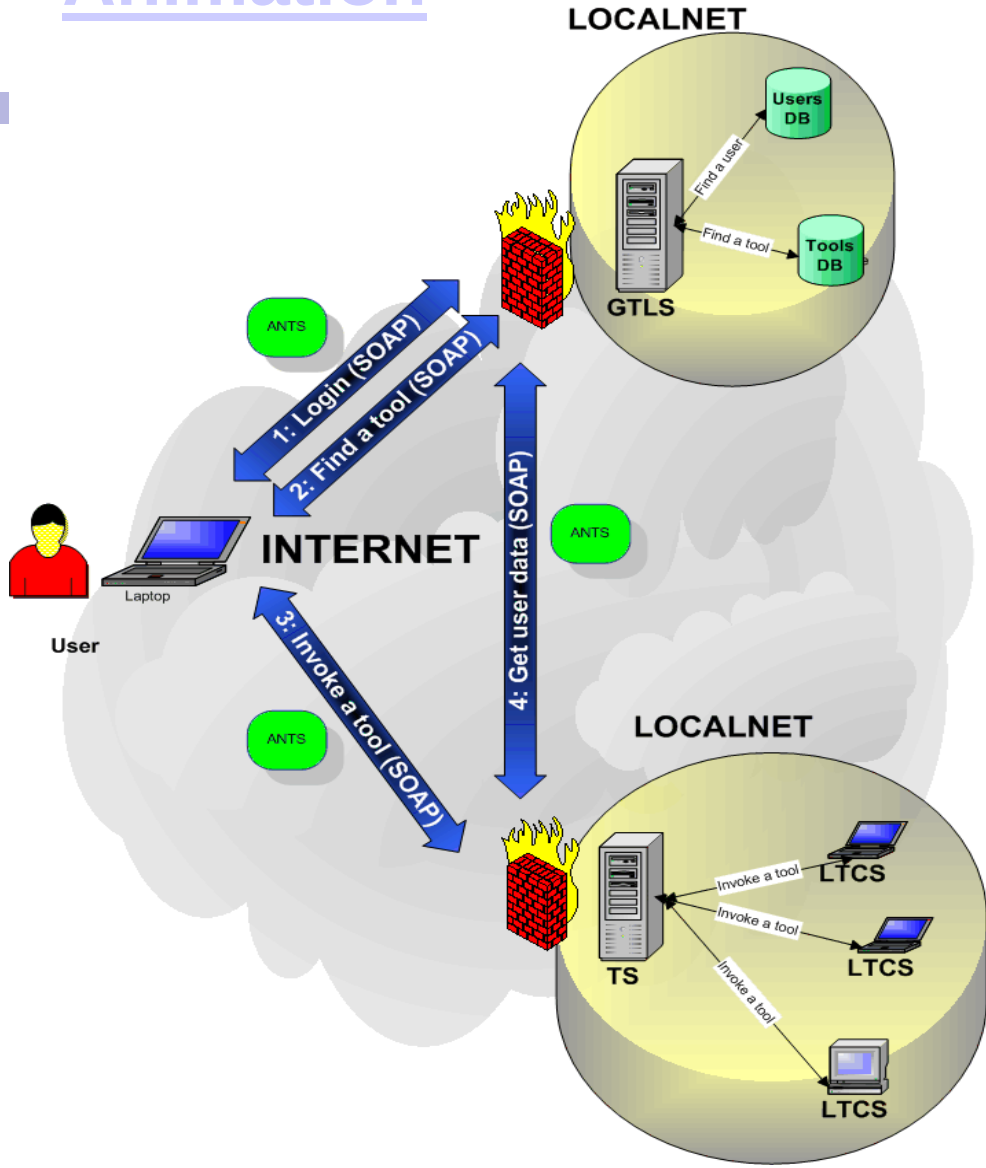


TRMS operation protocol

Animation

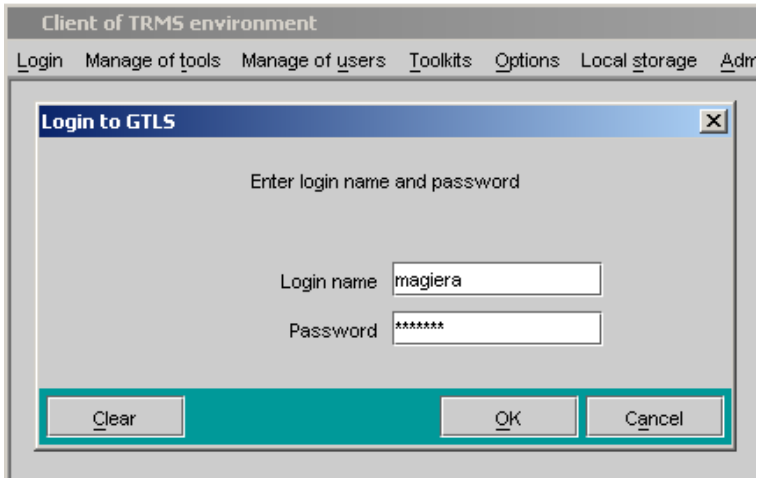
1: tool registers with profile

2: user asks for tool with constraints
3: registry checks constraints and returns profile
4: user lunches tool with input and output
5: tool fetches input and processes output
6: destination fetches output



Access control and Authorization in TRMS

- Access control and Authorization provide mechanisms to allow TRMS to restrict access to resources :

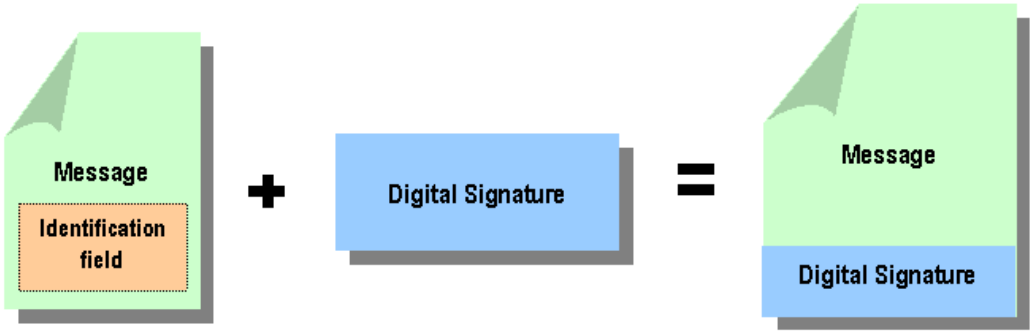


- login and password of user are verified on a central server of the TRMS environment (GTLS)
- complex privileges mechanism - permission to invoke specified tools, new tools registration, management of users ... are defined

- Additionally user's privileges could be confirmed by Tool Server (TS) in the course of the tool start-up.

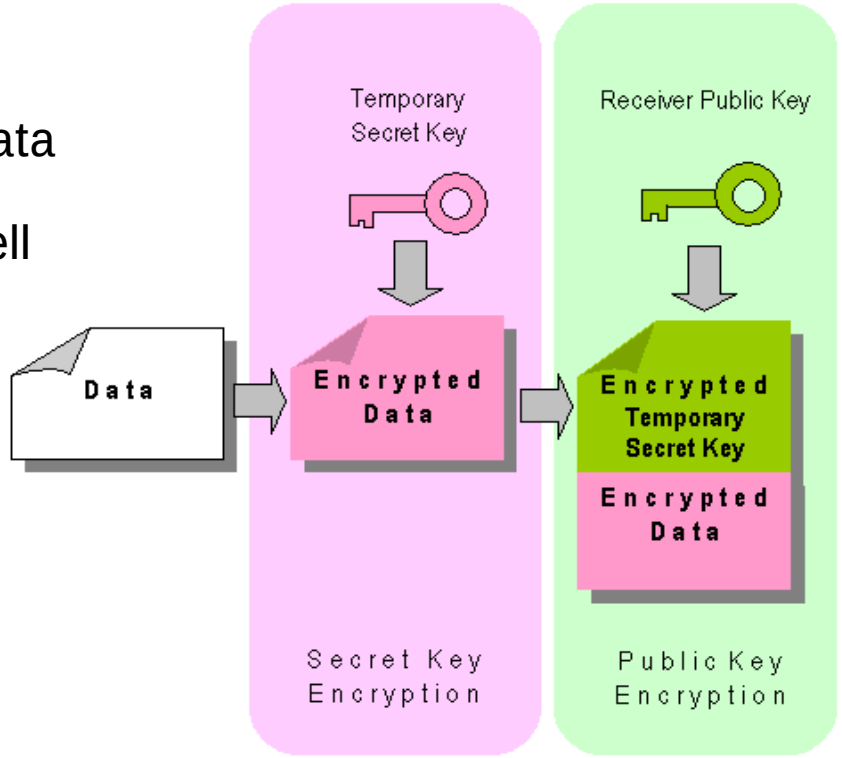
Authentication in TRMS

- Authentication constitutes a process by which we verify that a sender really is whom he claims to be. In TRMS this identification is achieved by the login process and by a digital signature.
  - Every message contains field identifying sender (login, SessionID)
  - Digital Signature of sender is affixed to each sent message



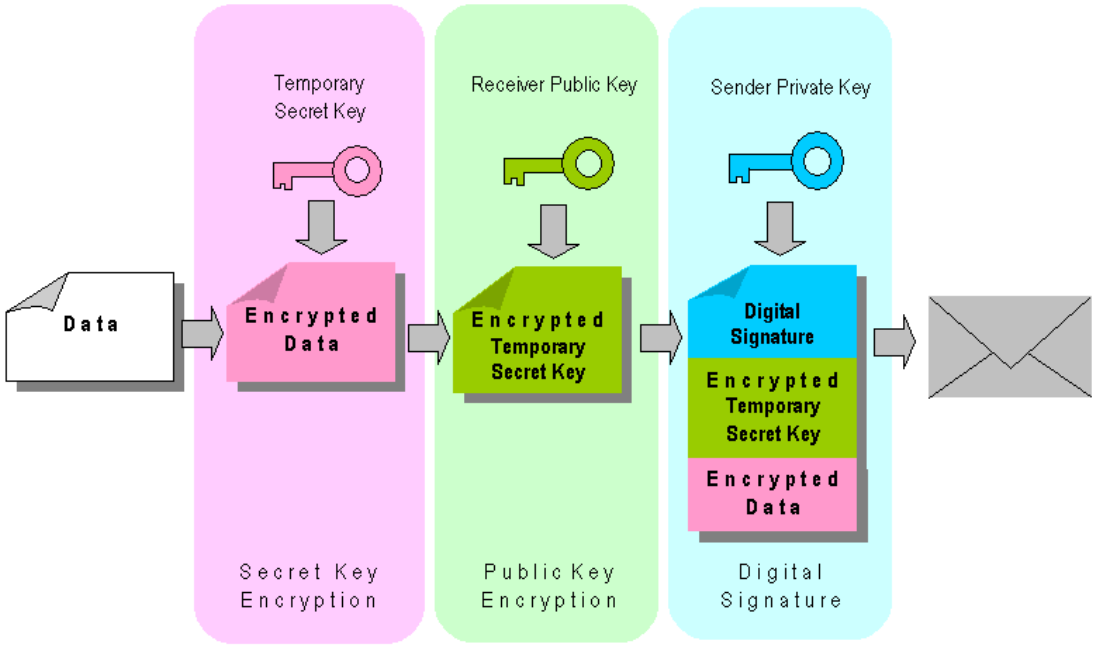
Confidentiality and integrity in TRMS

- Confidentiality and integrity assure that design data transported among distributed design teams are inaccessible for other and were not intercepted or changed on their way.
  - Confidentiality and integrity of data are achieved by cryptography methods.Secret key methods, as well as public key methods are used simultaneously.



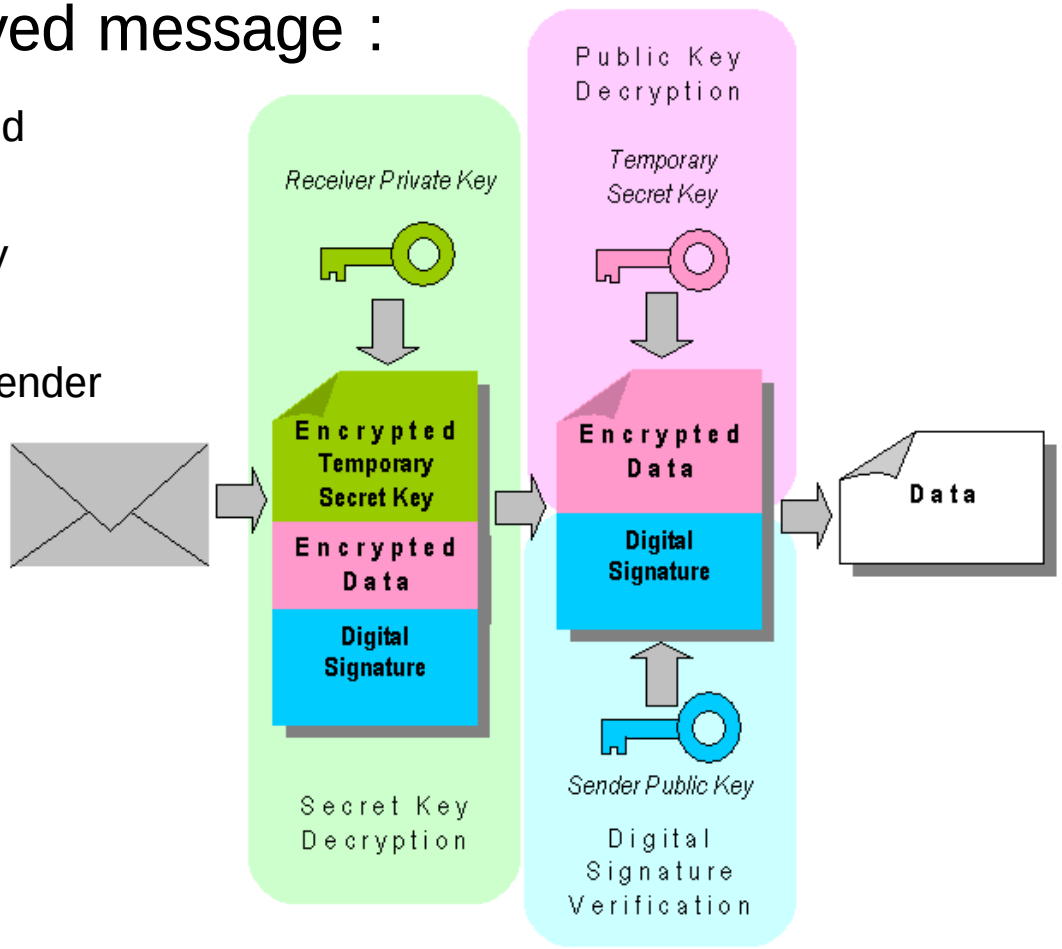
Preparation of a message for dispatch

- Preparation of a message for dispatch :
  - Temporary secret key is generated
  - Data is encrypted with temporary secret key
  - Temporary secret key is encrypted with receiver public key
  - Digital Signature is created with sender private key
  - Message is sent to receiver

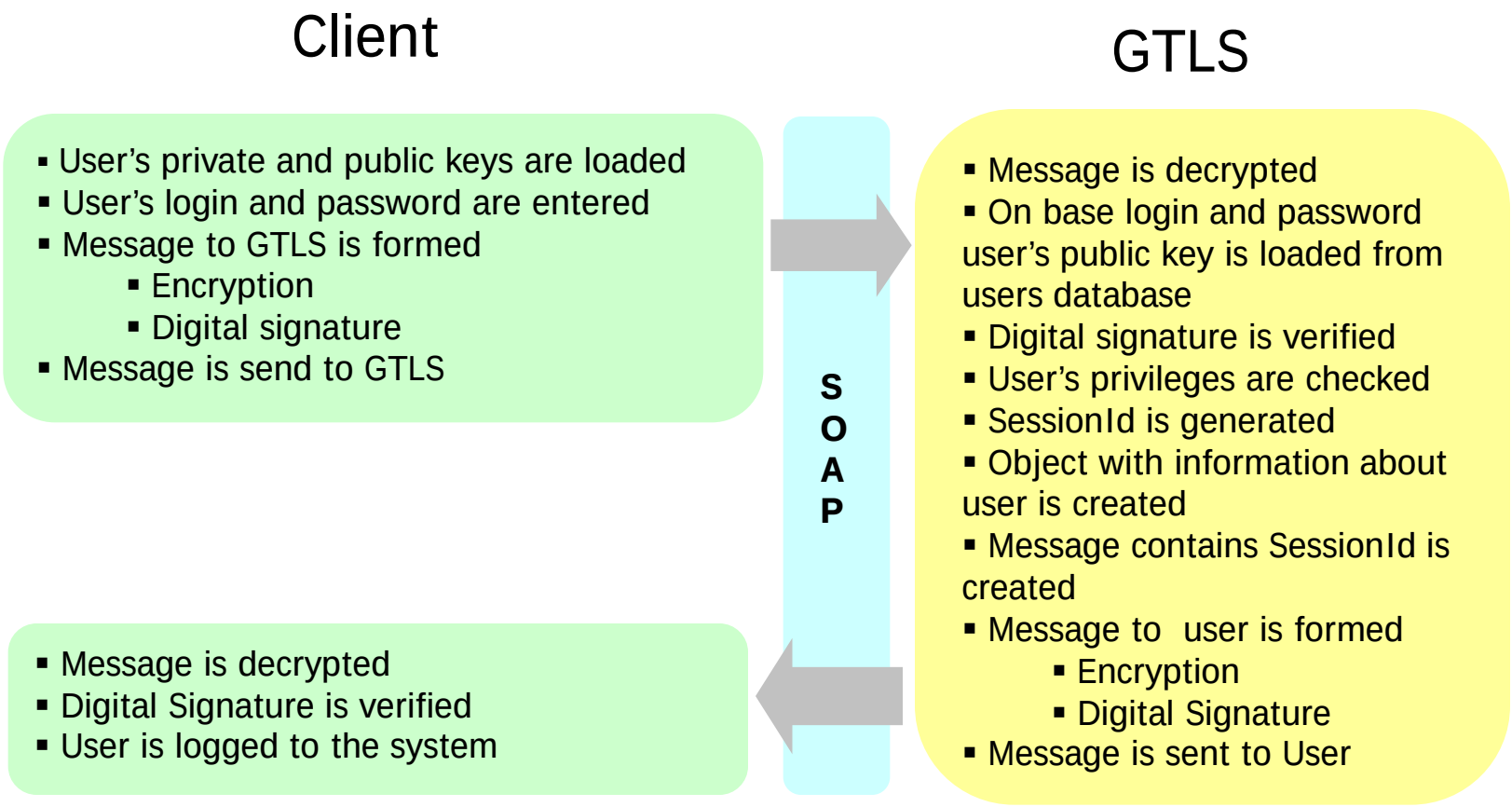


Decomposition of received message

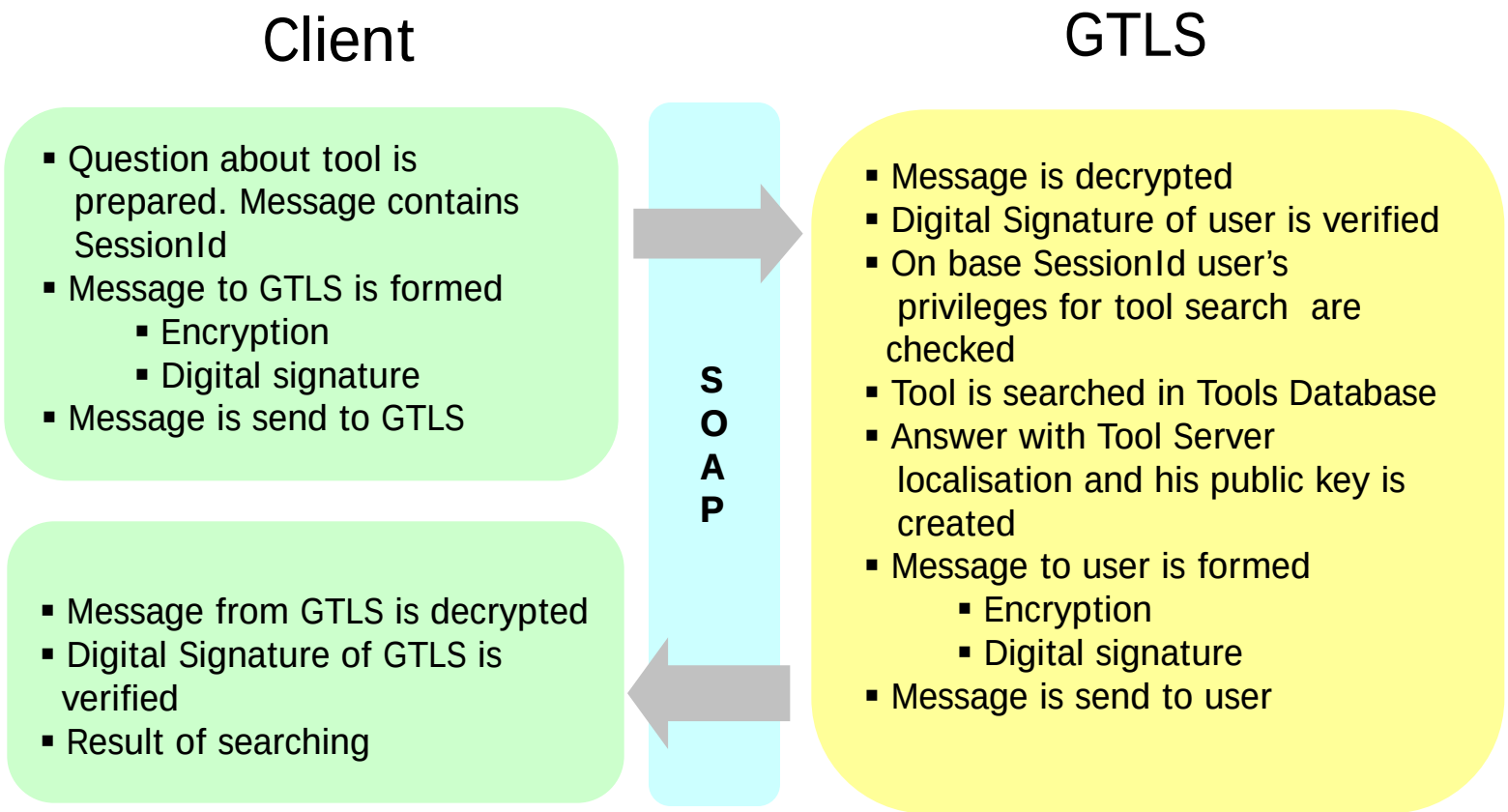
- Decomposition of received message :
  - Temporary secret key is decrypted with receiver private key
  - Data is decrypted with temporary secret key
  - Digital Signature is verified with sender public key



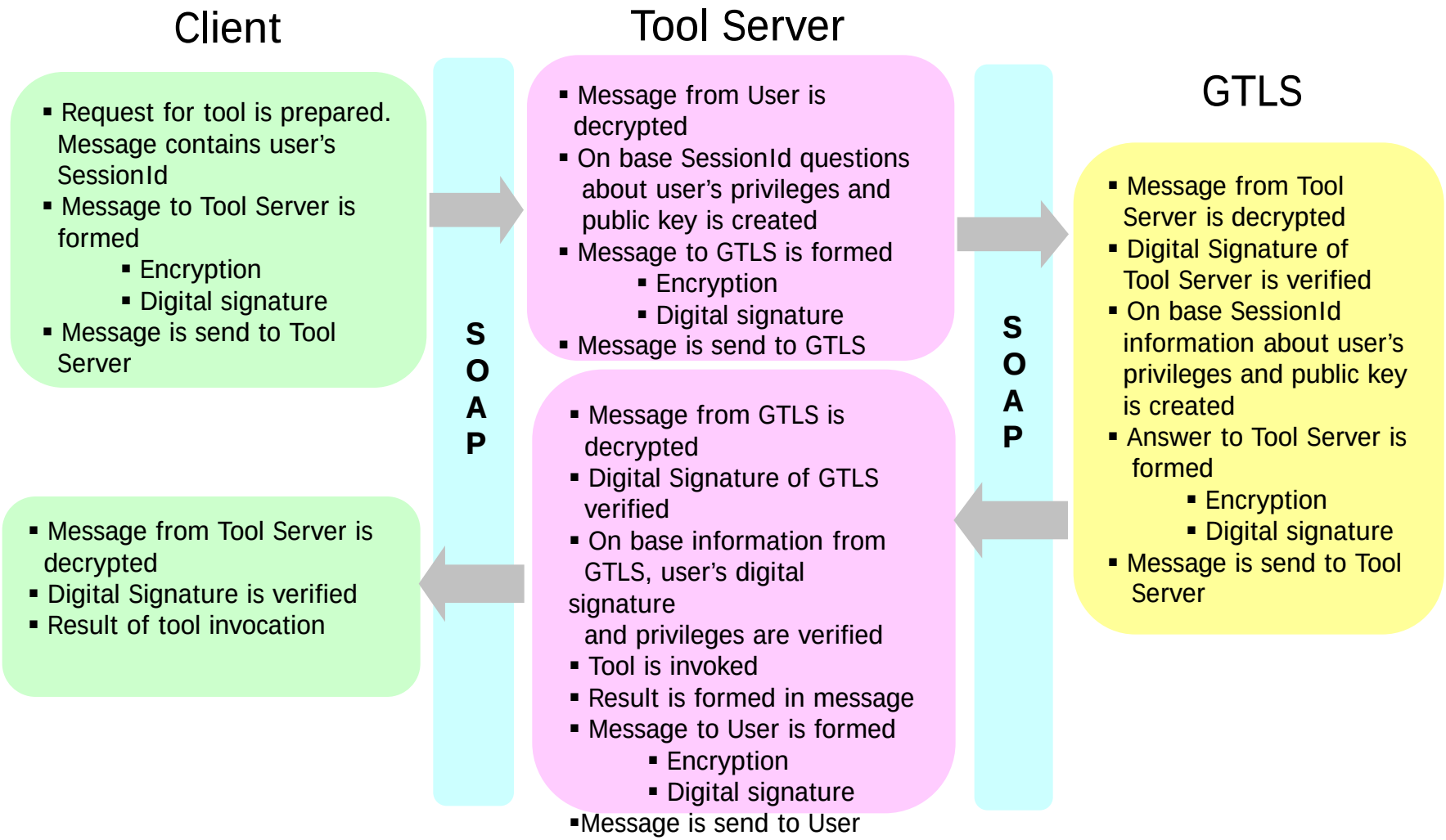
User login scenario



Tool invocation scenario 1/2



Tool invocation scenario 2/2



TRMS development summary

- TRMS is developed in Java 2 SDK 1.4.1 platform
  - Java cryptography architecture (JCA) includes a provider architecture that allows for multiple and interoperable cryptography implementations.
  - Java Cryptography Extension (JCE) is a set of packages that provides a framework and implementations for encryption, key generation and digital signature. The JCE is released separately as an extension to the SDK, in accordance with U.S. export control regulations.
- Cryptography methods and digital signature technology are applied
  - Cryptography methods :
    - Secret key method : Advanced Encryption Standard (AES) with key length 128 bits
    - Public key method : RSA Algorithm with keys length 1024 bits
  - Digital Signature:
    - MD5 with RSA Algorithm

Advantages of security mechanisms implemented in TRMS, 1/2

- Secure communication is assured by encryption algorithms directly built-in into application. Secret key algorithm as well as the public key algorithm are used simultaneously. It is not necessary to use other solutions such as SSL/TSL Protocol or VPN.
- User's private key is stored in a file protected by a password. In the future smart cards could be used.
- Login/password and digital signature are used for authentication.
- Extended and flexible system of privileges exists, which allows to furnish user with adjusted range of rights essential for realisation of project tasks.

Advantages of security mechanisms implemented in TRMS, 2/2

- User' rights to common resources are verified at least twice.
- Collaboration through existing firewalls is possible. Modification firewall rules limiting transmission of data is not indispensable. It is assured by Advanced Network Transport Service (ANTS).
- Mechanisms for security management give a system administrator a capability to force an appropriate behaviour of users.

TRMS vs. VPN

TRMS

- Establishes a secure tunnel between TRMS system components that exchange data. Data confidentiality and integrity is assured.
- All security mechanisms are built into the application. No need for additional components.
- Used 80 port is usually open. If not then ANTS component enables collaboration through a firewall without changing any firewall setting.
- Client stores his pair of keys (private and public) A public key of the central GTLS server is stored by the client program. These three keys are sufficient for TRMS use.
- A user may log into the system from any machine that has the TRMS client program.

VPN

- Establishes a secure tunnel between points that exchange data. Assures confidentiality and integrity of data.
- Realized, either in HW or SW.
- Influences the security policy. Requires changes in firewalls configuration that allow creation of a tunnel.
- Creates a „gate” in a protection system of the company. If a security policy of the accessed through the tunnel organization is less restrictive, a potential source of threat is established.
- With a large number of created VPN connections, a large number of used and stored keys may create a problem with their protection and management.

TRMS implementation

- TRMS is developed in Java 2 SDK 1.4.1 platform
  - Java cryptography architecture (JCA) includes a provider architecture that allows for multiple and interoperable cryptography implementations.
  - Java Cryptography Extension (JCE) is a set of packages that provides a framework and implementations for encryption, key generation and digital signature. The JCE is released separately as an extension to the SDK, in accordance with U.S. export control regulations.

- Cryptography methods and digital signature technology are applied
  - Cryptography methods :
    - Secret key method : Advanced Encryption Standard (AES) with key length 128 bits
    - Public key method : RSA Algorithm with keys length 1024 bits

Conclusions

- Securing CEEs/VEs is a complicated process, where application of proper technical, legal and organizational solutions are required
- Various available security measures enable to fit solutions to the organization activity nature
- Establishing and maintaining the assumed security level is not a single act but a continuous process requiring constant attention

Conclusions

- **TRMS limitations:**
  - Simplified workflow
  - Relatively slow data transmission (ANTS)
  - Support for teamwork is still rather limited
  - TRMS prototype needs more deployments

- **TRMS further R&D plans:**
  - Advanced Workflow Management System with enhanced editor
  - Smooth integration of the distributed tools layer with a communication layer of human actors (engineers)

    The E-Colleg collaborative engineering environment needs to be extended with advanced tools for synchronous and asynchronous communication of engineering team members
  - Measuring the engineering productivity increase is still a challenge
  - Social dimension in CEEs

Acknowledgement

The presented work has been done within projects:

- **E-COLLEG** (IST-1999-11746), and
- **VOSTER** (IST-2001-32031).

E-COLLEG partners are acknowledged for their R&D efforts in respect to the presented collaborative infrastructure.

- Dr. Wolfgang Mueller and Tim Schattkowsky, C-Lab (Univ. Paderborn),
- Dr. Matthias Bauer (Infineon Technologies),
- Siegfied Bublitz (Siemens Business Services)
- Dr. Manuel Carballeda (Thales Optronique SA). and
- Dr. Krystyna Siekierska (Institute of Electron Technology).

I acknowledge also Jarosław Magiera from CiEL/SUT group who has contributed to the security solutions in TRMS and other key developers of TRMS, namely: Paweł Fraś, Tomasz Kostienko, and Marek Szlęzak.

More information

on E-Colleg results is available on:

www.ecolleg.org

Including:

- TRMS demo
- TRMS documentation
- E-Colleg project papers and demonstrations

VOSTER web page **voster.vtt.fi**

VE Forum **www.ve-forum.org**

Thank you for your attention!