Sead Muftic
Security Framework for Development of Secure Network Applications

E-mail: sead.muftic@setecs.com
Office: (202) 994 – 5506
Cell: (240) 535 – 2095
July 30, 2003

PKI, Smart Cards and Crypto Functions

Current Situation

Problem:
- Development and deployment of secure network applications
- Complicated, expensive, long
- Compliance to standards and interoperability
- Not transparent and user-friendly

Solution:
- Security Framework: collection of ready-made components (objects) for common PKI, smart cards, and crypto functions and protocols

Security Framework:
- Concept (how to solve the problem)
- Methodology (approach to use the concept)
- Set of components (Dev Toolkit, plus run-time platform)
Secure Applications

Secure applications:
1. SETECS ready-made applications
2. Third-party development (new applications)
3. Existing (standard) applications

OneNET – Drop-Down Menus

Development of Customized Applications
Integration with Internet Explorer

Encrypted and Signed Software Modules

Conclusions

Security Framework:

- Concept (how to solve the problem)
  By creating a set of generic security modules for the most common security components, functions, and protocols and integrating them with existing (standard) and new (custom-developed) applications

- Methodology (approach to use the concept)
  Templates for new applications, procedure for integration with standard applications, and transparent invocation

- Set of components (Dev Toolkit, plus run-time platform)
  Crypto objects, security protocols, ready-made client/server components, and several available applications