Welcome to PKCS ’99

Royal Institute of Technology, Stockholm
29 September – 1 October 1999

RSA SECURITY

Agenda

- **Recent developments, work in progress, future directions for the Public-Key Cryptography Standards**
- **Wednesday:**
  - **Prof. Johan Håstad, KTH**
  - **PKCS #5, #12, Contributors' Agreement, #9, #11**
  - **product demonstrations**
- **Thursday:**
  - **PKCS #1, #14, #15**
  - **interoperability workshop**
- **Friday:**
  - **PKCS #13, ASN.1, new work items**

RSA SECURITY

PKCS Distinctives

- **Purpose:**
  - catalyst for formal and *de facto* standards
  - "missing pieces"
- **Scope:**
  - public-key infrastructure, as well as cryptography
- **Process:**
  - "informal," "intervendor"

RSA SECURITY

RSA Security Inc.

- New name for merger of three companies:
  - Security Dynamics Technologies (Bedford, MA, USA)
  - RSA Data Security (San Mateo, CA, USA)
  - Dynasoft AB (Stockholm, Sweden)
- Three business lines:
  - RSA SecurID: strong authentication
  - RSA BSAFE: PKI components
  - RSA Keon: advanced PKI solutions
- RSA Laboratories is the advanced technology and standards development group

RSA SECURITY

Workshop Representation

- As of last Wednesday, among the 38 designating a country in our “informal” registration process ...
  - Austria, France, Ireland, Israel, Japan, Taiwan (1 ea.)
  - Finland (2)
  - Canada, UK (3 ea.)
  - Germany, USA (4 ea.)
  - Sweden (16)
- Current registration is ~56

RSA SECURITY