Metering
A Pre-pay Technique

Russell Housley
SPYRUS Chief Scientist

housley@spyrus.com

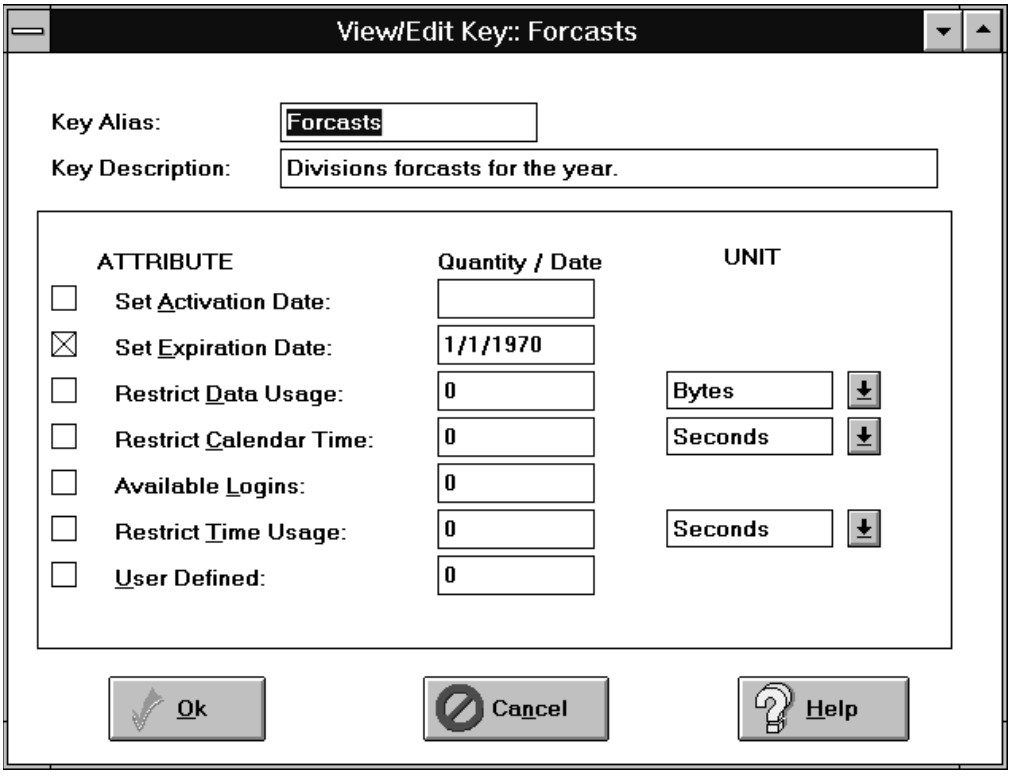
SPYRUS Metering System

- SUPPLIER ENCRYPTS INTELLECTUAL PROPERTY AND SETS CONTENT-BASED METERS
- TOKENS CONTAIN CRYPTOGRAPHIC KEYS AND THEIR ASSOCIATED METERS WHICH CONTROL THE USE OF THE KEYS
    - SYMMETRIC KEYS
    - ASYMMETRIC KEYS
- CRYPTOGRAPHIC HARDWARE CONTAIN REAL TIME CLOCK
- INFORMATION CAN ONLY BE ACCESSED IF THE METER CONSTRAINTS ARE MET

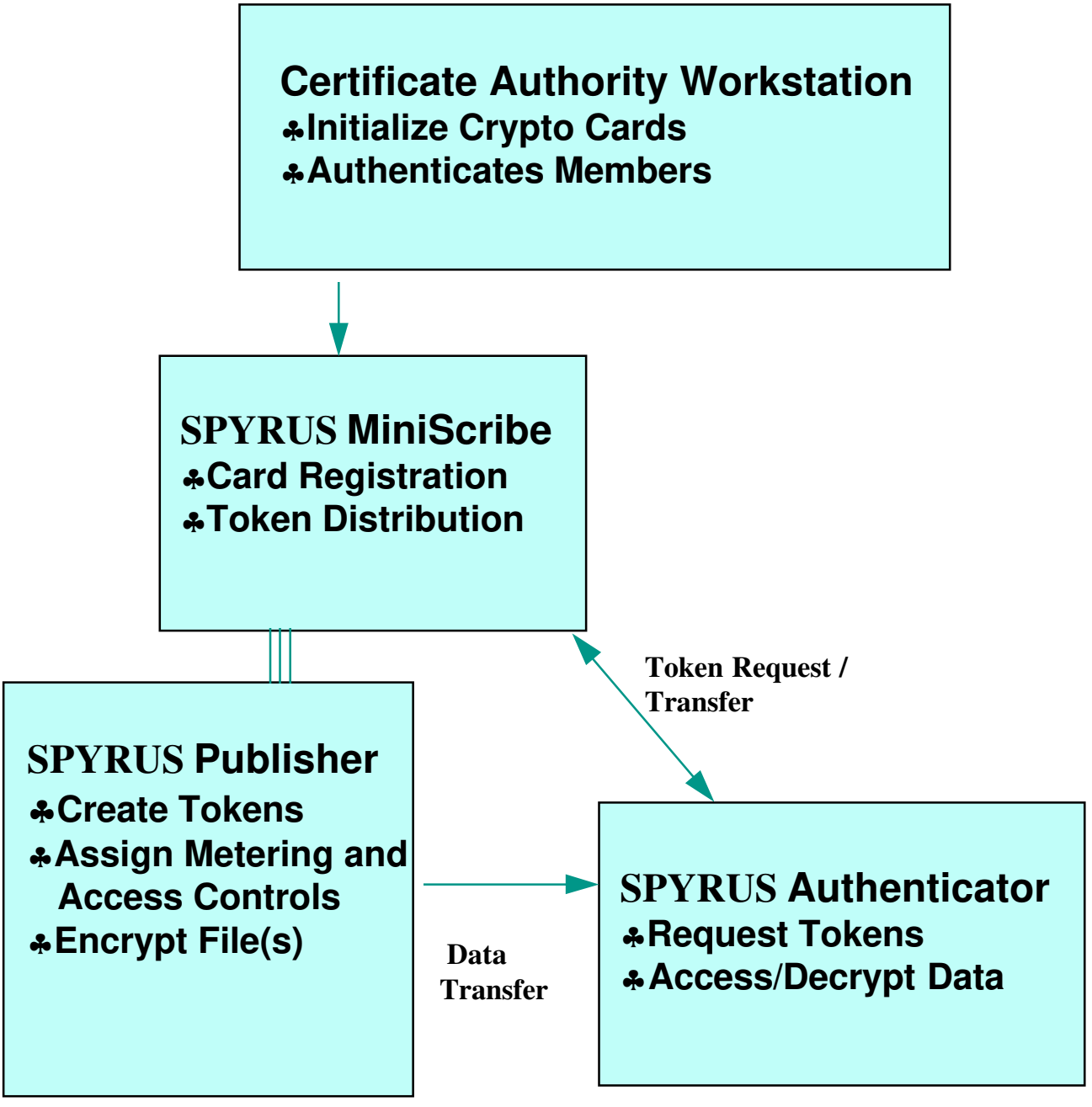
Token Attributes

- NAME (ALIAS) ASSOCIATED WITH THIS KEY
- DESCRIPTION OF THIS SECURITY KEY
- ACTIVATION DATE OF THE KEY
- EXPIRATION DATE OF THE KEY
- NUMBER OF USES OF THE KEYS
- DATA USAGE
- TIME ACCESS
- CALENDAR TIME ACCESS
- OTHER -- LYNKS AWARE APPLICATIONS

Token Attributes



System Components



Binding Tokens

- **THE PUBLISHER DETERMINES HOW MUCH DATA IS PROTECTED WITH A EACH KEY**
  - **SINGLE FILE**
  - **WHOLE DIRECTORY**
  - **ARBITRARY COLLECTION OF FILES**
  - **WHOLE VOLUME OR CD-ROM**
  - **OTHER ...**

- **METERS ARE NOT JUST FOR DATA**
  - **METER SIGNATURE KEY USAGE**
  - **METER PHYSICAL ACCESS TO A LABORATORY**

Subscriptions

- CRYPTOGRAPHIC KEY UPDATES CAN BE USED TO IMPLEMENT A SUBSCRIPTION SERVICE
- EACH ISSUE IS PUBLISHED UNDER A DIFFERENT KEY
- A ONE-WAY UPDATE FUNCTION IS APPLIED TO THE FIRST KEY TO OBTAIN THE SECOND KEY, AND SO ON...
- THE METER CONTAINS THE NUMBER OF UPDATES THAT ARE PERMITTED
- ALLOWS A SUBSCRIBER TO ENTER THE SYSTEM AT ANY ARBITRARY POINT

Time Enforcement

- **DATE / TIME METERS ARE ENFORCED WITHIN CRYPTOGRAPHIC HARDWARE**
- **HARDWARE CONTAINS A REAL TIME CLOCK FOR A RELIABLE, "TRUSTWORTHY" TIME SOURCE**
- **CRYPTOGRAPHIC OPERATIONS FAIL IF THE TIME CONSTRAINTS WITHIN THE METER ARE NOT SATISFIED**

Payment = Key Management

- KEYS WITH ASSOCIATED METERS ARE DISTRIBUTED AFTER PAYMENT IS RECEIVED
- "TRY BEFORE YOU BUY" IS SUPPORTED
  - LIMIT ACCESS TO NON-PRIME TIME
  - LIMIT ACCESS TO A SUBSET OF AVAILABLE DATA
  - FULL ACCESS, BUT RESTRICT DECRYPT QUANTITY
  - RESTRICT NUMBER OF DATABASE QUERIES
- PAYMENT CENTER CAN BE MAINTAINED BY THE PUBLISHER OR PROVIDED AS A SERVICE
- PAYMENT CENTER CONNECTED TO VARIOUS DATABASES OFFER MANY FLEXIBLE ALTERNATIVES

Worked Example: CD-ROM

- ISO 9660 (CD-ROM) IMAGE ENCRYPTION
- SPYRUS AUTHENTICATOR
  - VERIFY PUBLISHER'S SIGNATURE ON CD-ROM
  - ALLOW USERS TO QUERY AN ENCRYPTED CD-ROM
    - TABLE OF CONTENTS
    - REQUIRED KEYS
  - REQUEST AND DOWNLOAD TOKENS FROM KEY DISTRIBUTION SYSTEM
- SPYRUS DECRYPTION DRIVER
  - TRANSPARENT DECRYPTION OF DATA
  - MULTI-PLATFORM SUPPORT (UNIX, PC WINDOWS)

PCMCIA
Security Working Group

- **CO-CHAIRS: SPYRUS AND IBM**
- **SCOPE:**
  - **DEFINE SECURITY CARD CLASS OF DEVICES**
  - **DEFINE CAPABILITIES AND REQUIREMENTS FOR NEW SECURITY CARD CLASS**
  - **UNDERSTAND THE ISSUES ASSOCIATED WITH SECURITY CARDS, INCLUDING HIGH ASSURANCE REQUIREMENTS FOR THE BANKING, FINANCIAL, AND COMMERCE COMMUNITIES**
  - **RECOMMEND CHANGES TO SPECIFICATIONS FOR SUPPORT OF SECURITY CARD CLASS**

PCMCIA Security Working Group Tasks

- **IMMEDIATE TASKS:**
  - **DEFINE AND ALLOCATE A DEVICE IDENTIFIER FOR SECURITY CARD DEVICES**
  - **DEFINE EXTENSIONS AND THEIR META-FORMATS**

- **OTHER TASKS:**
  - **COUNTERMEASURES FOR SOPHISTICATED ATTACKS**
  - **PROTECTION FROM ILL BEHAVED APPLICATIONS**
  - **ISSUES OUTSIDE THE SCOPE OF PCMCIA CARD AND SOCKET SERVICES**