

# Dynamic Cryptographic Context Management

Trusted Information Systems, Inc.

Dr. Dennis Branstad and David M. Balenson, Principal Investigators

Sponsored by the

High Confidence Networks Program

DARPA Contract # F30602-97-C-0277

Hilarie Orman, Program Manager

Mike Ferenti, Rome Laboratory, Contract Specialist

Captain Robert (Steven) Durst, Contract Officer Technical Representative

# Objectives

- Identify/create practical cryptographic key management methods for efficiently changing the key(s) protecting a multi-participant application when participation changes rapidly;
- Define protocols for initiating, negotiating, establishing, and managing secure sessions among changing groups of authorized participants;
- Produce and demonstrate software toolkits that implement a selected key management method and negotiation protocol in both a group manager's workstation and up to 100,000 user workstations.

# Consultants

- Dr. Yvo Desmedt (University of Wisconsin)
  - Dynamic Group Keying Methods
- Dr. John McHugh (Portland State University)
  - Dynamic Group Communications Methods
- Dr. Ray Sidney (RSA Laboratories)
  - Dynamic Group Keying Protocols

# Advisors

- Dr. David Aucsmith (Intel Corporation)
  - Common Data Security Architecture
- Dr. Gus Simmons (Sandia Laboratories, Retired)
  - Dynamic Group Threat Analysis
- Mr. Carl Campbell (Mastercard International)
  - Large Group Key Update Protocols

# Funding

- By Year

– FY 97	218,039
– FY 98	550,000
– FY 99	<u>334,701</u>
	1,112,740

- By Cost

Labor (+ overhead)	917,584
Consultants	46,000
Travel	36,152
Equipment	40,000
Fee	61,484
Cost of Money	<u>11,520</u>
	1,112,740

# Tasks/Deliverables

- Documentation
  - Research Reports
    - Multi-Party Application Security Requirements (5)
    - Dynamic Multi-Party Crypto Context Management Architecture and System Design (5)
    - Multi-Party Cryptographic Context Template (12)
    - Multi-Party Cryptographic Context Negotiation Protocol (16)
    - Dynamic Cryptographic Context Management Project Evaluation (24)
  - Administrative Reports
    - Program Progress Reports (Quarterly)
    - Contract Funds Status Reports (Quarterly)
    - Presentation Material (i.e., Briefing) Slides (5 days before meeting)

# Tasks/Deliverables (contd.)

- Software Generation/Demonstration
  - Project Kick-Off Meeting (1)
  - Software Product Specification (22)
  - Dynamic Cryptographic Context Negotiation (Software) Toolkit (22)
  - Software Toolkit Familiarization Session (22)
  - Dynamic Cryptographic Context Management Demonstration (24)

# Analysis Subtasks

- Select multi-party applications of interest
- Identify/collect security requirements for selected applications
- Investigate group communication protocols (broadcast, multi-cast, any-cast)
- Investigate security policy language requirements for security manager use
- Analyze cryptographic keying methods for large-group applications

# Synthesis Subtasks

- Define initial security negotiation template
- Select/create security policy specification language and translator
- Specify translation of security policies to crypto context using initial template
- Create multi-party key specification, selection, initialization, update, and destruction protocols

# Development Subtasks

- Create manager-workstation software for policy, template, authorization, initialization, negotiation functions
- Create user-workstation software for template, initialization, authentication, negotiation functions

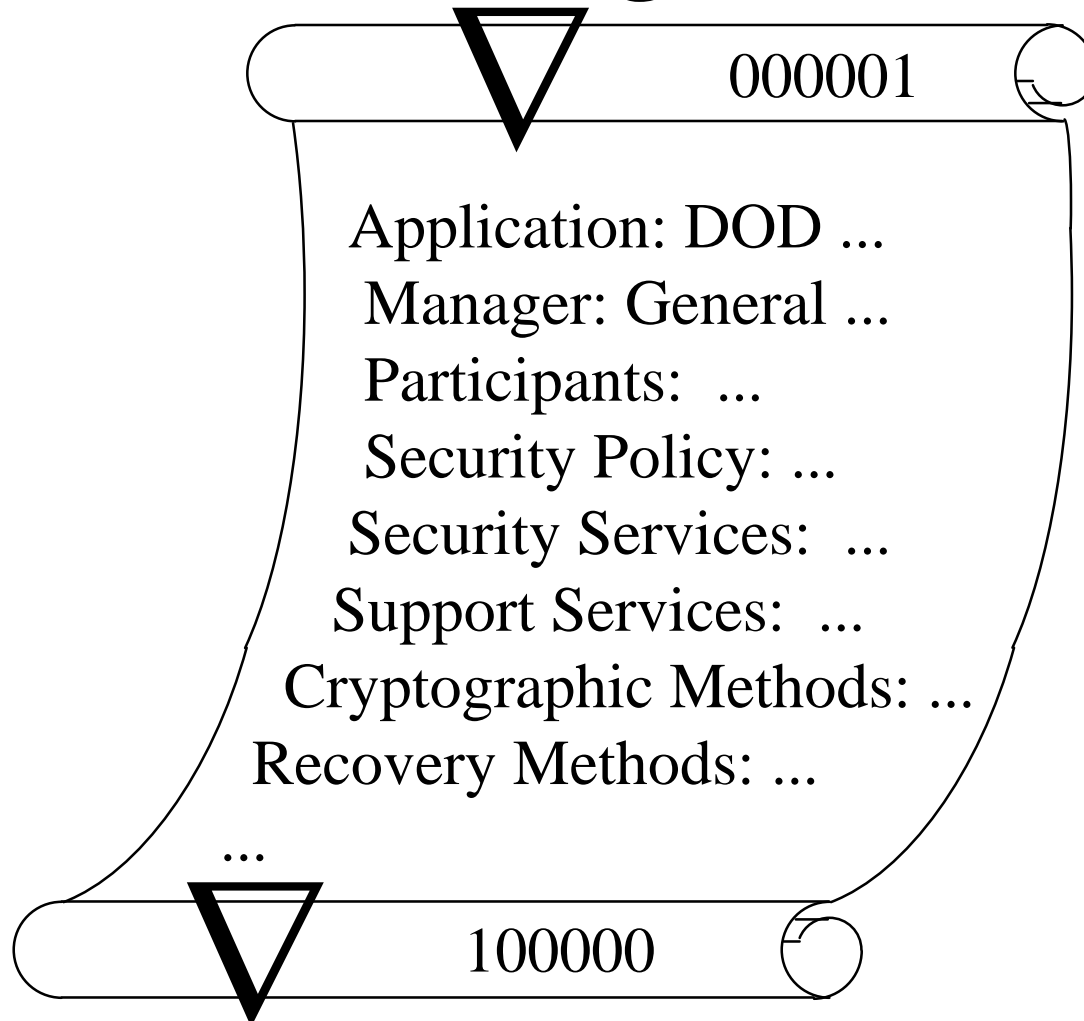
# Demonstration Subtasks

- Specify security policy for application in manager workstation (MWS)
- Specify authorized group for application (MWS)
- Translate security policy to context selection using template (MWS)
- Determine set of available participants and authenticate them

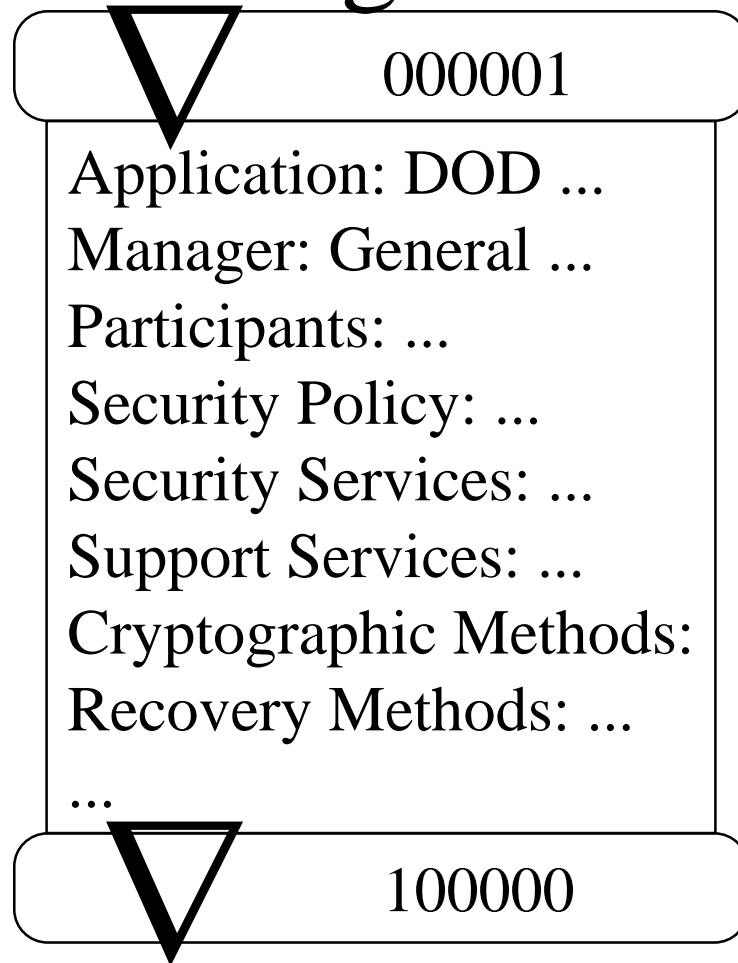
## **Demonstration Subtasks (contd.)**

- Negotiate security/crypto context with available participants from authorized group (MWS and UWS)
- Establish initial security association/session (MWS and UWS)
- Add participant when requested  $\Rightarrow$  update key
- Delete participant when exiting  $\Rightarrow$  update key
- Maintain log of session (participants, activity)
- Disconnect session when done

# Dynamic Cryptographic-Context Management

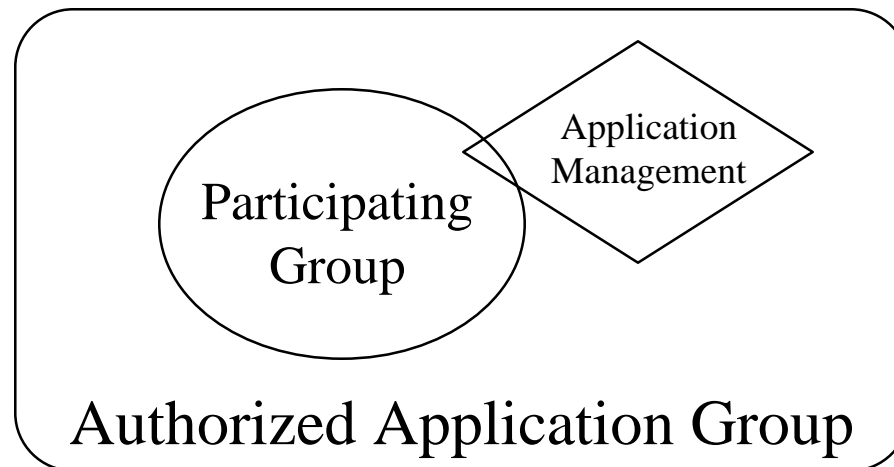


# Dynamic Cryptographic-Context Management



# Dynamic Group Requirements

- Application management changes
- Authorized application group changes
- Group manager changes aperiodically
- Participating group changes dynamically



# Large-Group Computer Applications

- Military Command and Control
- Simulated War Games
- Large-Scale Collaborative Designs
- International Medical Research Consortium
- Distributed Computer Conferencing

