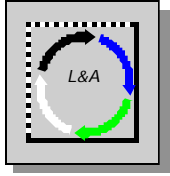


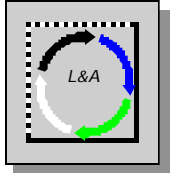
# **CRYPTOGRAPHY: BOARDROOM BUZZWORD**

Sandra M. Lambert  
1997 RSA Data Security Conference  
January 30, 1997



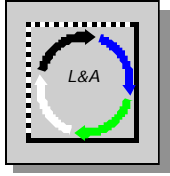
## **ICC/BIAC/OECD Business-Government Forum on Global Cryptography Policy**

- Meeting held May 7, 1996 in Washington, D.C.
- Summary of recent meetings on cryptography policy since prior forum
- Updates on cryptography policy development from governments: France, U.K., E.C., U.S., Japan, Germany
- Summary of BIAC/ICC Joint Discussion Paper on International Cryptography Guidelines presented as possible starting point for business and government to reach consensus on issues



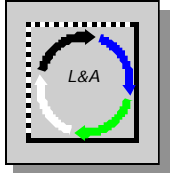
## **ICC/BIAC/OECD Business-Government Forum (Cont.)**

- 4 Panels
  - Government access issues
  - Key management policies
  - Liability issues of key holders, owners and governments
  - Global availability and implementation of cryptographic methods
- Drafting process for OECD Guidelines



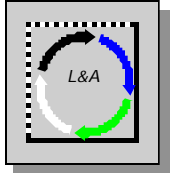
## **Ad Hoc Group of Experts on Cryptography Policy Guidelines**

- Created in March 1996 as a subgroup of the Group of Experts on Security, Privacy & Intellectual Property Protection in the GII
- Mission: develop cryptography guidelines by February 1997
- Meeting held May 8, 1996 in Washington, D.C
- Attendees: EC, BIAC, OECD Secretariat, government representatives from Australia, Austria, Canada, Denmark, France, Germany, Japan, Norway, Spain, Sweden, Turkey, U.K. and U.S.



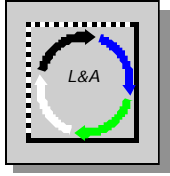
## **Ad Hoc Group Of Experts (Cont.)**

- Format of document: non-binding OECD recommendations or guidelines so as to not affect the sovereignty of OECD Member Countries. They will be a framework for national policies and international cooperation.
- General recognition of the importance of including business in the discussions and the impact of government decisions on business



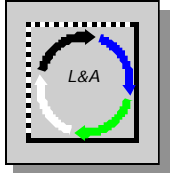
## Ad Hoc Group Of Experts (Cont.)

- Utilized BIAC/ICC Joint Discussion Paper on International Cryptography Guidelines as basis for discussion
  - Scope
    - \* Address individuals' as well as business' interests
    - \* Exclude cryptography for protecting national security purposes where national security products do not include commercial off-the-shelf products
    - \* Audience for paper: governments, business, citizens



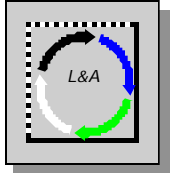
## **Ad Hoc Group Of Experts (Cont.)**

- Definitions
  - \* Taken from ISO and reviewed to determine adequacy and relevance
  
- General Recognition
  - \* Building an effective GII and providing for its security is a principal goal
  - \* Balance between national sovereignty and international cooperation is important
  - \* Governments have obligations to foster privacy and commerce as well as law enforcement



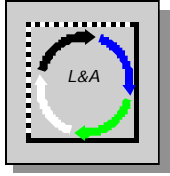
## **Ad Hoc Group of Experts (Cont.)**

- \* Government access is necessary. The central question is whether we are going to promote government access products through voluntary and market-based measures, or not.
- \* No agreement on extent of government role in establishing quality control of security products
- \* Reference should be made to the 1980 OECD Guidelines on the Protection of Personal Data and Transborder Data Flows to the extent appropriate
- \* Include a standard phrase throughout the document about the need for strong cryptography for GII and commerce



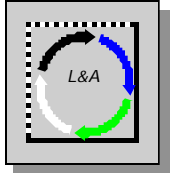
## **Ad Hoc Group of Experts (Cont.)**

- Principles
  - \* No specific agreements were reached on the language of the nine principles
- OECD Secretariat distributed a summary of the meeting
- OECD Secretariat inserted specific comments/suggestions of Member Countries into the BIAC/ICC Joint Discussion paper and circulated to the Ad Hoc Group prior to the next meeting in June
- Prior to the June meeting, some countries submitted formal statements on their country views or approach to encryption policy



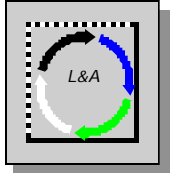
## **Ad Hoc Group of Experts (Cont.)**

- Meeting held June 26, 27 in Paris
  - Revised version of the guidelines was reviewed
- Meeting held September 26, 27 in Paris
  - Various issues within the guidelines were discussed and one principle was added
- Meeting held December 16 - 20 in Paris
  - Guidelines were finalized



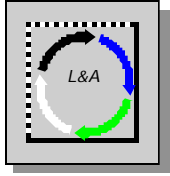
## **Ad Hoc Group of Experts (Cont.)**

- Three documents were produced
  - \* Cover Memorandum to the Council
  - \* Recommendation of the Council Concerning Guidelines for Cryptography Policy
  - \* Annex to the Recommendation of the Council Guidelines for Cryptography Policy
- Proposed Narrative Report on Cryptography was eliminated
- Recent developments....



## Other OECD Efforts

- Paper entitled “Electronic Commerce: Opportunities and Challenges for Governments and Firms” was drafted
  - Role of governments with respect to electronic commerce
  - Recent developments....



## **USCIB Response to Draft Paper “Enabling Privacy, Commerce, Security and Public Safety in the GII”**

- Developed by the Information Policy Committee
- Contained comments on:
  - Main principles or themes contained in the paper
  - Various points in the paper compared to the October 1994 USCIB Business Requirements for Encryption
  - The six specific actions in the paper
  - Digital signature vs. encryption infrastructure
- Provided input and influence to future direction