GAMMA

ISO/IEC 17799

Information Security Management
Application to Smart Cards

by Dr. David Brewer

Gamma Secure Systems Limited

Diamond House, 149 Frimley Road
Camberley, Surrey, GU15 2PS +44 1276 702500
dbrewer@gammassl.co.uk

Agenda

- What is it?

- How does it work?

- MRA and certification

- Benefits
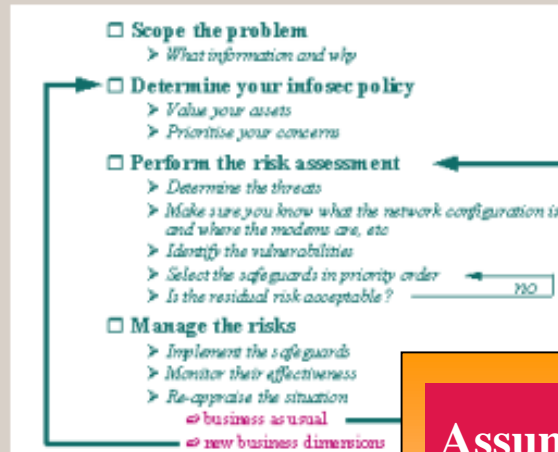
- Application to smart cards

What is it?

- IS 17799 is a *catalogue of good things to do*

- BS 7799 Part 2 is a *specification for an ISMS (Information Security Management System)*

- There are a number of certification schemes

Effective Security

How does it work?

The means by which management can monitor and control information security, to reduce the business risk to an acceptable level and ensure that security continues to fulfil their corporate, customer and legal

□ Scope the problem
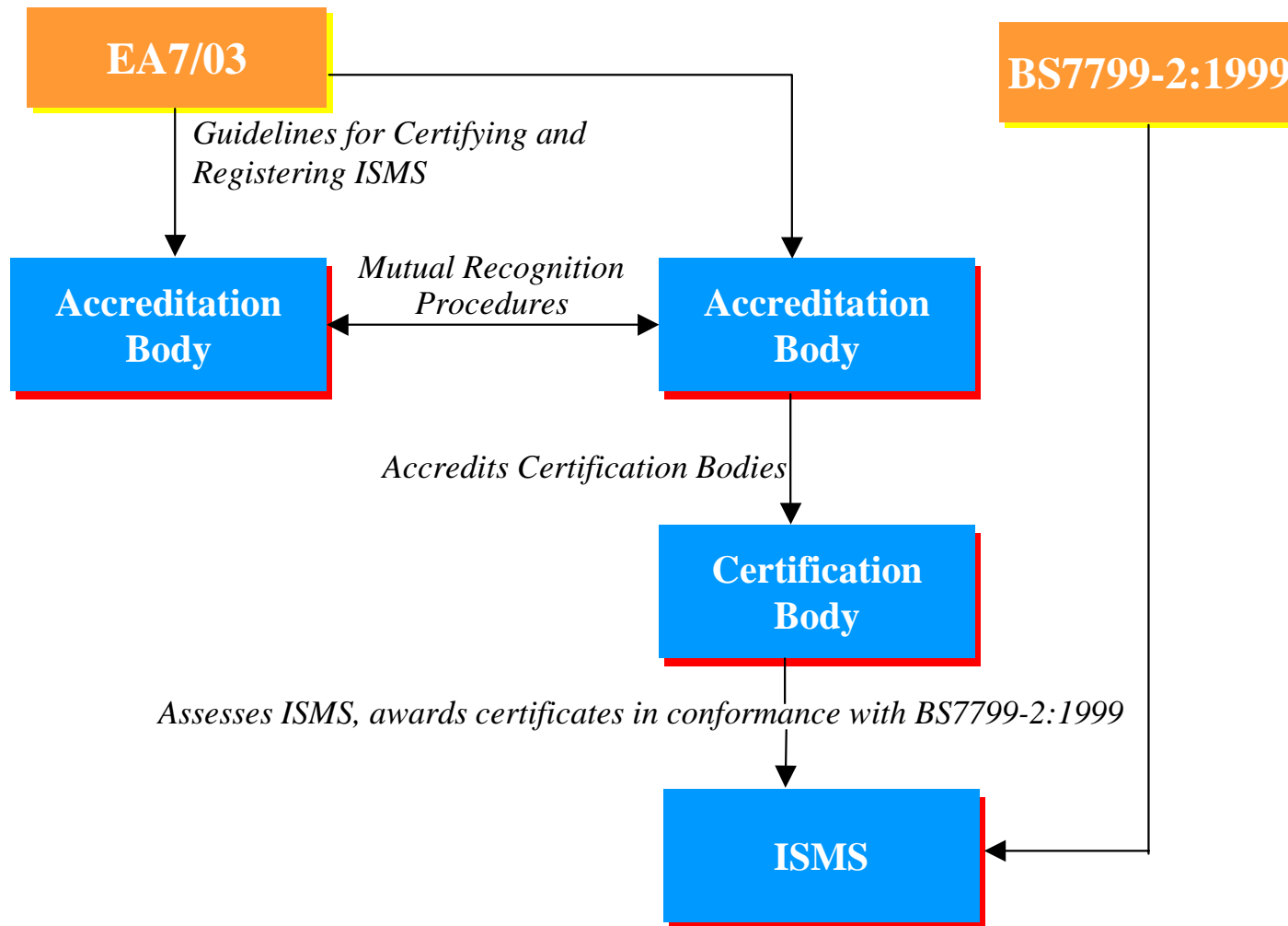 ➤ What information and why
□ Determine your infosec policy
  ➤ Value your assets
  ➤ Prioritise your concerns
□ Perform the risk assessment
  ➤ Determine the threats
  ➤ Make sure you know what the network configuration is and where the modems are, etc
  ➤ Identify the vulnerabilities
  ➤ Select the safeguards in priority order
  ➤ Is the residual risk acceptable?   no
□ Manage the risks
  ➤ Implement the safeguards
  ➤ Monitor their effectiveness
  ➤ Re-appraise the situation
    ➪ business as usual
    ➪ new business dimensions

Check in place & is it effective?

Assumptions

BS 7799 Controls

Residual Risks

Monitor and control

Continues to be acceptable

MRA and Certification

EA7/03

BS7799-2:1999

Guidelines for Certifying and Registering ISMS

Accreditation Body

Mutual Recognition Procedures

Accreditation Body

Accredits Certification Bodies

Certification Body

Assesses ISMS, awards certificates in conformance with BS7799-2:1999

ISMS
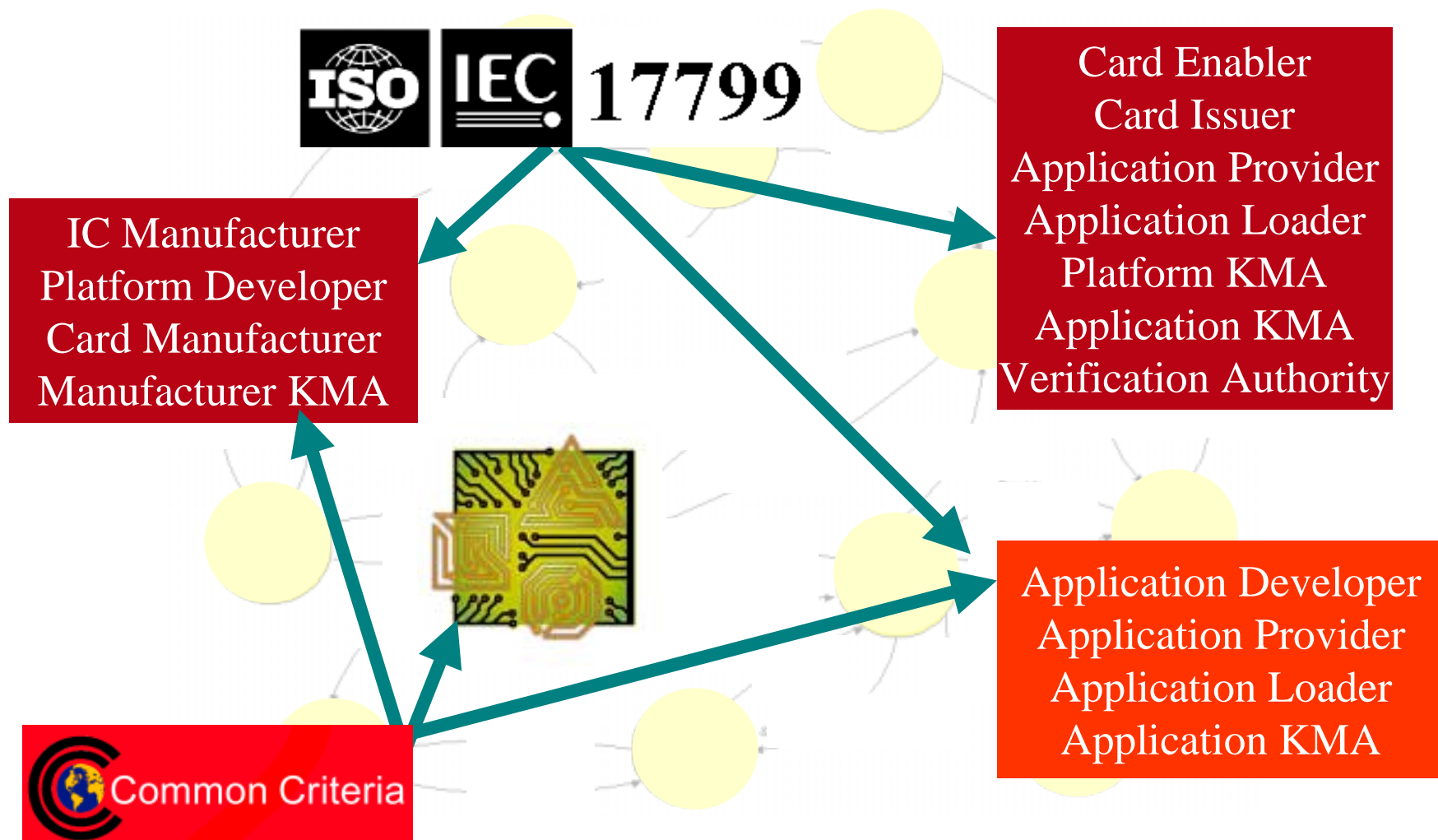
Benefits

▌ Integrates security with business processes

▌ Turns security into a business enabling process

▌ Provides a standard framework for managers to monitor and control

▌ Promotes the competence, security-wise, of a company to its market

▌ Reduces the need for customers to check for themselves

Application to Smart Cards

ISO IEC 17799

IC Manufacturer
Platform Developer
Card Manufacturer
Manufacturer KMA

Card Enabler
Card Issuer
Application Provider
Application Loader
Platform KMA
Application KMA
Verification Authority

Application Developer
Application Provider
Application Loader
Application KMA

Common Criteria

For Further Information

(c) Gamma Secure Systems Limited, 2001