security **consulting**

What about the ITSEC?

logica

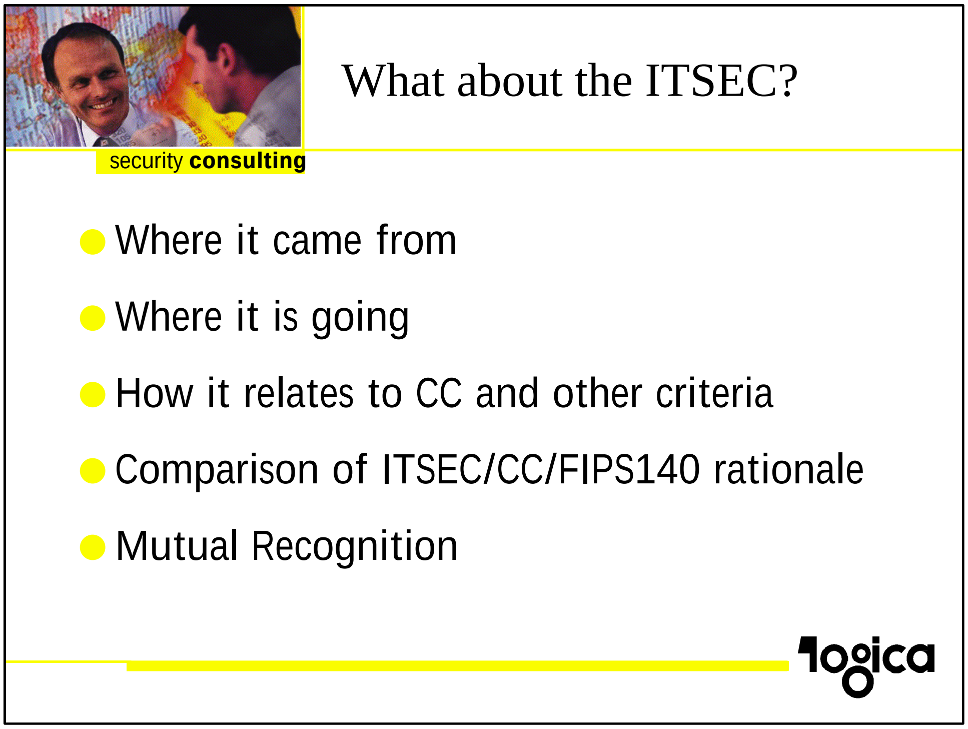
This presentation is part of the 4th CACR Information Security Workshop.

The presentation discusses why the ITSEC is still relevant as well as how experience from the ITSEC has contributed towards the current position with evaluations.

In such a short presentation it is not possible to go into much detail on any part of the subject. There are, therefore, approximations made in this presentation - it should not be used as a definitive source of information.

Logica is an independent IT Services company employing over 8800 staff world-wide and operating in 26 countries.

Andy Webber, Logica.
mailto:webbera@logica.com
http://www.logica.com
to April 2000 - +44 171 446 4201
from April 2000 +44 20 7446 4201



security **consulting**

What about the ITSEC?

- Where it came from
- Where it is going
- How it relates to CC and other criteria
- Comparison of ITSEC/CC/FIPS140 rationale
- Mutual Recognition

The ITSEC has been around for most of the decade. It has been overtaken by the Common Criteria so surely it is old news?

Since there is a vast investment in any 3rd party evaluation and a significant lead time from development to certification, there will continue to be ITSEC evaluations being performed for some time to come. In addition, developers with experience of ITSEC are likely to continue to use it as their default criteria as they climb the learning curve of the Common Criteria for future evaluations.

The ITSEC will therefore be around for some years to come. Indeed, although the UK ITSEC Scheme has in place procedures for migration to CC evaluations, it is still open to new evaluations to both the ITSEC and the CC.

The ITSEC and CC have a fundamentally different approach to evaluation compared to the Orange Book and FIPS 140 assessments. An understanding of the ITSEC can help to understand the meaning of parts of the CC.

Before the ITSEC, there was no formal recognition of any security evaluations in other nations (that I am aware of). One of the reasons for developing the joint or harmonised criteria of the ITSEC in Europe was to promote the mutual recognition of certificates. Although a long, slow and legally fraught path, this was achieved. The lessons from this process have helped the CC to get to the position that it is, with 6 nations signed up to the Mutual Recognition Arrangement.

security **consulting**

Where it came from

- UK (mainly government) criteria
- German criteria
- French and Dutch proposals
- Proposed new UK criteria
- European harmonisation ...

There were a number of criteria that had been developed in Europe. These all took a different approach to the Orange Book. The European criteria were all based on the need for flexibility - a capability to to evaluate security functionality specified to meet a variety of security problems. The European criteria therefore took an approach of defining what properties of the target of evaluation had to be examined to obtain assurance.

The UK's CESG (Communications-Electronics Security Group) had defined their criteria and evaluation methods in Memo 2/Memo 3 and Manual A.

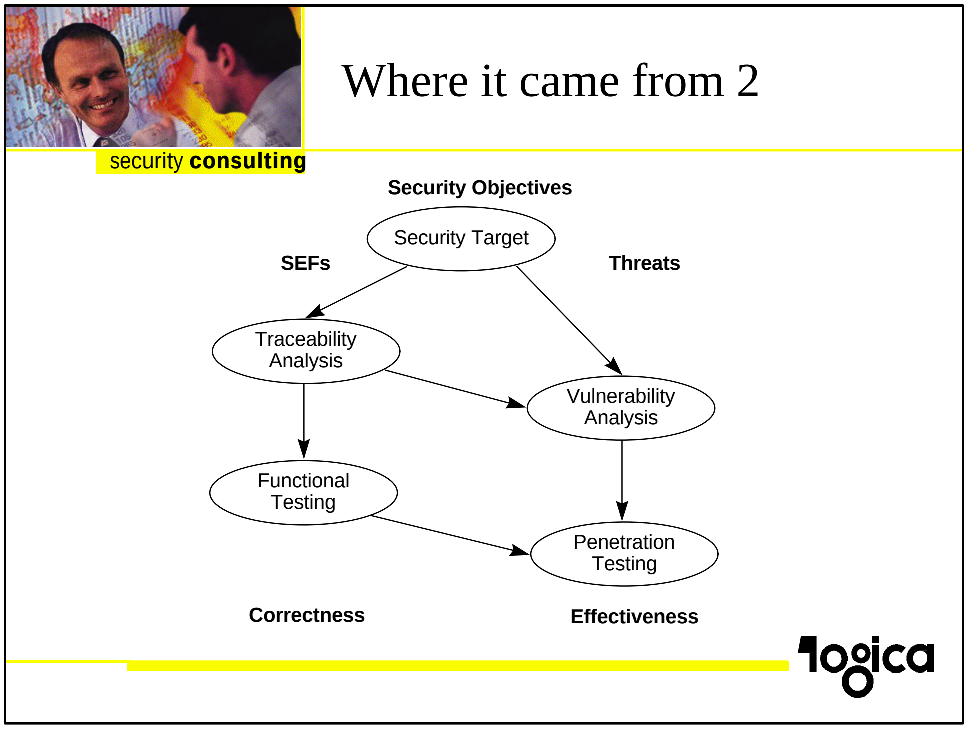
The German's BSI (Bundesamt für Sicherheit in der Informationstechnik) had defined their criteria in their Criteria for the Evaluation of Trustworthiness of Information Technology Systems.

The French SCSSI (Service Central de la Sécurité des systèmes d'Information) were in the process of drafting their Catalogue de Critères Destinés à évaluer le Degré de Confiance des Systèmes d'Information.

The Dutch were also drafting criteria.

In the UK, as part of a move away from evaluations purely for the Government's benefit, work was underway on a 'new' criteria by the DTI (Department of Trade and Industry).

Within Europe it became clear that all the concepts of evaluation were similar across Europe, and that efforts to draft and update criteria should be co-ordinated. The result was the ITSEC and ITSEM.



Where it came from 2

security **consulting**

Security Objectives

Security Target

SEFs

Threats

Traceability Analysis

Vulnerability Analysis

Functional Testing

Penetration Testing

Correctness

Effectiveness

The ITSEC has a fundamental concept of a split between Correctness and Effectiveness.

The correctness aspect is mainly based on validation and verification techniques following the process of refinement (e.g. waterfall model of development) of the Security Enforcing Functions (SEFs) through the design and, depending on the E level, to the code. In all cases, this is supported by functional testing which aims to demonstrate the the functions/features are present an operating correctly.

The effectiveness aspect can be thought of in a number of ways, including:

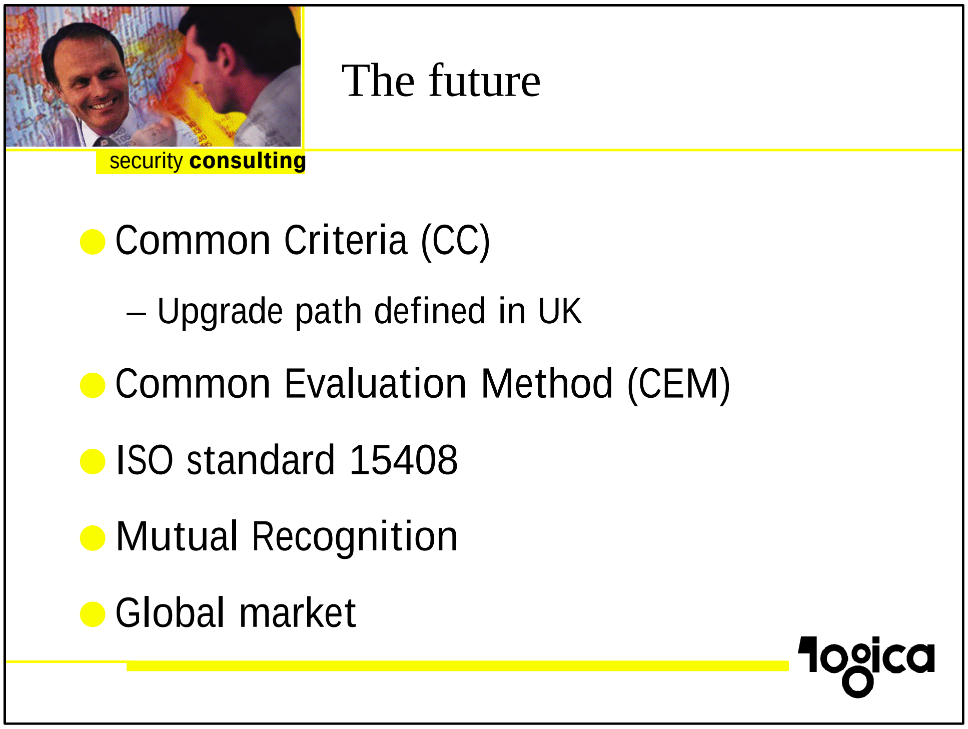
• Ensuring that in the refinement process, sight has not been lost of the purpose of the security features (i.e. to counter the threats)

• Considering all the ways that the (correct) functions cannot be bypassed, circumvented, directly attacked, indirectly attacked or otherwise overcome in contravention of the security policy/features

• Answering the question "what could possibly go wrong?"

Effectiveness analysis takes in all the information about potential vulnerabilities gleaned from the correctness aspects. It culminates in penetration testing, where theories about potential vulnerabilities are proved or disproved.

The Effectiveness analyses are divided up into portions like Binding Analysis, Strength of Mechanisms etc. However, this is mainly to ensure that each of the key aspects is covered in the totality of the analysis. It is not considered important to pigeon-hole a problem.



security **consulting**

The future

- Common Criteria (CC)
  - – Upgrade path defined in UK
- Common Evaluation Method (CEM)
- ISO standard 15408
- Mutual Recognition
- Global market

logica

The ITSEC is gradually being replaced by the Common Criteria as the preferred criteria of evaluation sponsors. There are however a number of reasons why the ITSEC will still be relevant for some time to come.

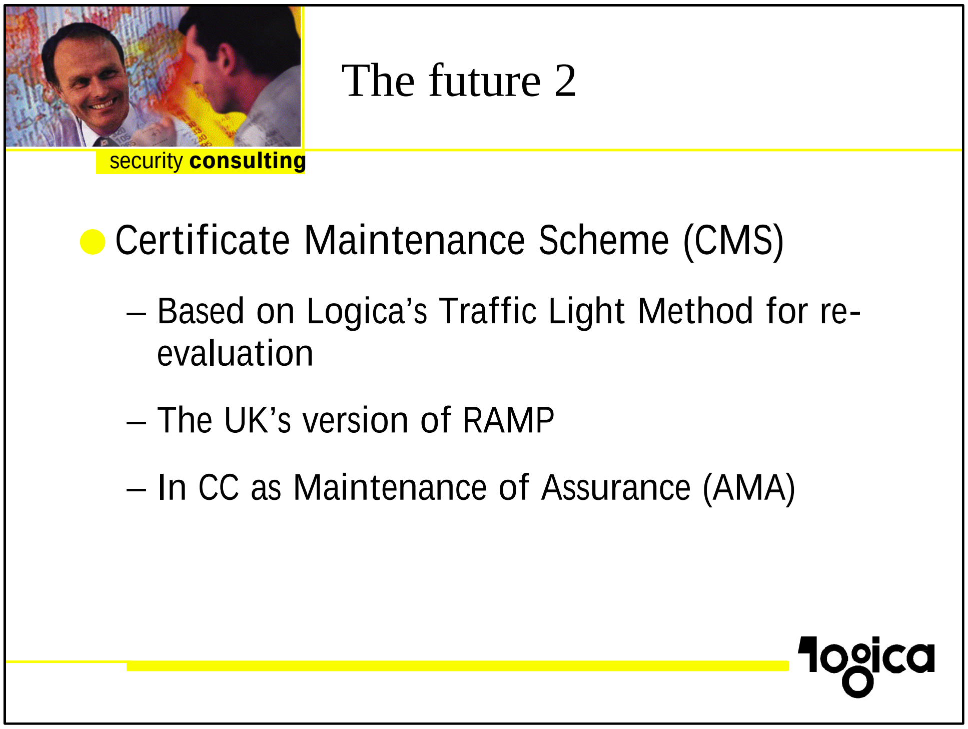
One of these is that there is a significant amount of investment and knowledge of the ITSEC. To some extent, the ITSEC represents a lower risk approach to evaluation (through past experience). In addition, in certain markets, the mutual recognition of ITSEC certificates is more valuable than the mutual recognition of CC certificates (e.g. high assurance levels and the European market).

In some countries (notably Germany) the ITSEC is referenced in legislation.

Ultimately, however, it is anticipated that the ITSEC will fall into disuse and will be formally dropped in favour of the CC. No dates have been set for this yet - market demand will determine the timescales.

The ITSEC was accompanied by the ITSEM which defined the (common parts of the) method for performing evaluations against the ITSEC. In the same way, the Common Evaluation Methodology (CEM) defines the methodology for CC evaluations.

As the CC becomes more widely used, it is expected that the existing ITSEC mutual recognition agreements will be reflected in the CC mutual recognition arrangement. This will help to define a single global marketplace for evaluation and evaluated products and systems.


security consulting

The future 2

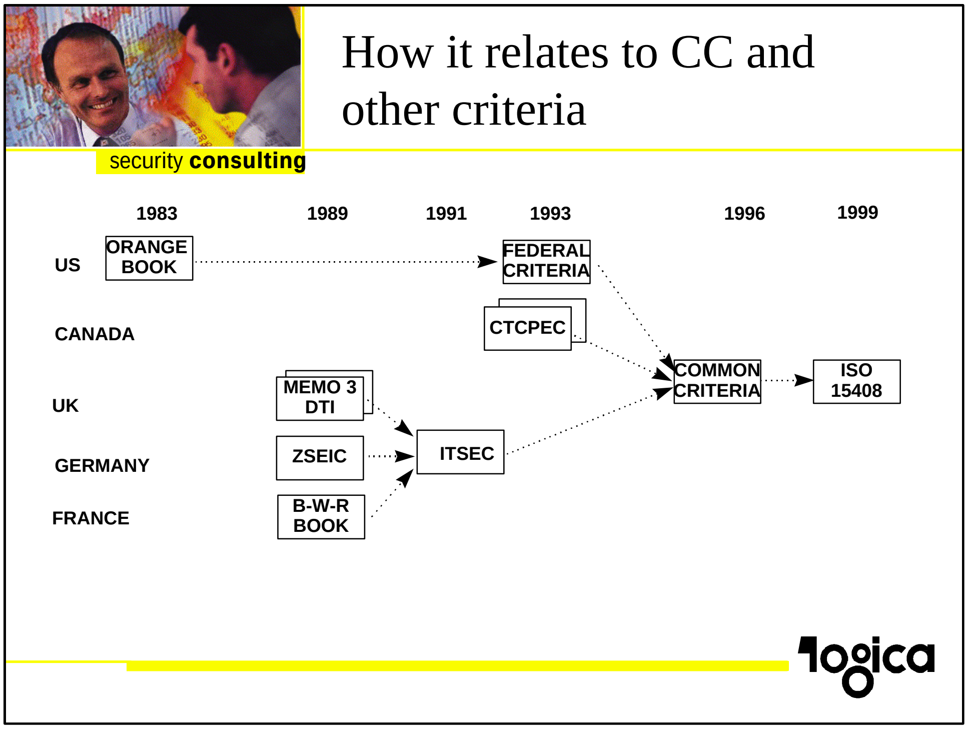
- Certificate Maintenance Scheme (CMS)
  - Based on Logica's Traffic Light Method for re-evaluation
  - The UK's version of RAMP
  - In CC as Maintenance of Assurance (AMA)

In the purest use of the documentation, if a product is changed, it must undergo the evaluation process again - all of it. Realistically it is possible to make use of a significant portion of previous evaluation results where they remain valid. The Traffic Light Method was a defined technique for determining the potential impact of changes on a product's ability to uphold the security requirements. It was called the Traffic Light method as there were 3 categories of change - Red for security critical, Amber (yellow) for potentially affecting security and Green for not affecting security. This categorisation can be applied at each representation, so for example, changing the source code (but not the design) of a security critical component requires that code to be re-examined and tested (with a consideration of knock-on effects). Changing the Security Target to add security features ripples down through the architecture, design and code.

CMS is an extension of the UK Scheme, like RAMP, to which defines the procedural and technical aspects of membership. The scheme helps developers keep their evaluated products both up-to-date and evaluated. It also helps them to manage changes in their product and minimise the impact on evaluation (costs and timescales).

The CC's AMA is comparable to both RAMP and CMS, although it introduces more flexibility.

Another reason that there will be ITSEC certificates for some time into the future is that developers with a heavy investment in the ITSEC and CMS are likely to migrate to the CC slowly.



How it relates to CC and other criteria

security **consulting**

1983 1989 1991 1993 1996 1999

US

ORANGE BOOK

FEDERAL CRITERIA

CANADA

CTCPEC

UK

MEMO 3 DTI

COMMON CRITERIA

ISO 15408

GERMANY

ZSEIC

ITSEC

FRANCE

B-W-R BOOK

logica

Note that this diagram is not to scale - dates are approximate and show published works.

The arrows show the primary despondency of the criteria. Inevitably, any criteria draws something from all previous criteria.

The diagram helps to show the origin of concepts. Each leaf-node introduced a new concept to evaluation or a different way of considering the security of a product/system.

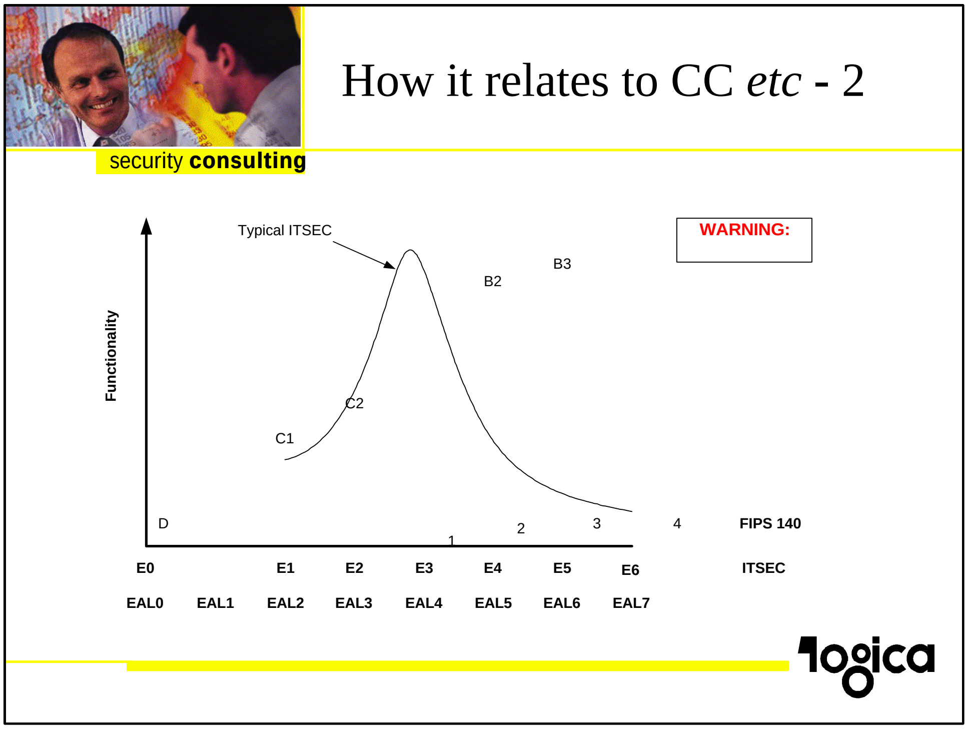
•Orange Book - specified functionality; TCB.

•Memo 3 - ‘any’ functionality; boundaries, gates & fence penetration.

•ZSEC - example functionality, effectiveness analysis, strength of mechanisms

•CTCPEC - component levelling and dependencies

•Federal Criteria - Protection Profiles



How it relates to CC *etc* - 2

security **consulting**

WARNING:

Again, this is not to scale. The question of how assurance maps to an absolute scale is one that will keep philosophers busy for a long time to come. Essentially, it is an increasing scale. Steps are not necessarily equidistant.

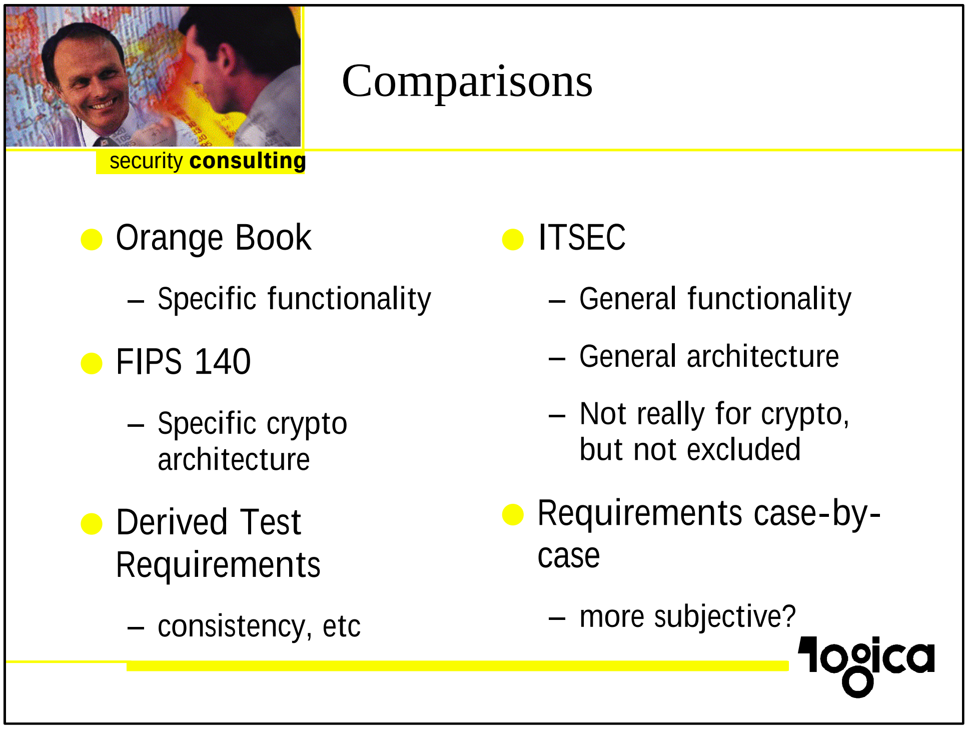
The curve shows approximately the amount of functionality that we typically see in ITSEC evaluations - there are always exceptions - this is just the typical.

Lower assurance levels are usually chosen by smaller vendors or for products where security is not the prime function, but where some assurance in the security is required. It is also used for low assurance security ‘bolt on’ products, like PC access control packages.

Medium assurance levels are often chosen by large vendors of general purpose IT products where a significant customer base is likely to use the security features (e.g. multi-user operating systems and databases). It also chosen for medium assurance security add-ons like Firewalls and mainframe domain partition facilities. Medium assurance products normally have security controls applied to general functionality which can be used in many ways.

High assurance levels are chosen where security is of paramount importance. The prime example of this is the One Way Regulator that only allows serial (RS-232) data to flow in one direction. More recent examples include smartcards designed to store real value and be used in potentially hostile environments - e.g. MAOSCO’s Multos and Mondex’s Purse.

The ITSEC curve can be explained by the fact that the cost of evaluation is roughly based on the product of assurance and functionality - more like f(functionality)*g(assurance).



Comparisons

security **consulting**

- Orange Book
  - Specific functionality
- FIPS 140
  - Specific crypto architecture
- Derived Test Requirements
  - consistency, etc

- ITSEC
  - General functionality
  - General architecture
  - Not really for crypto, but not excluded
- Requirements case-by-case
  - more subjective?

logica

The left hand side highlights the “American approach” where the criteria contain specific details about how things should be done.

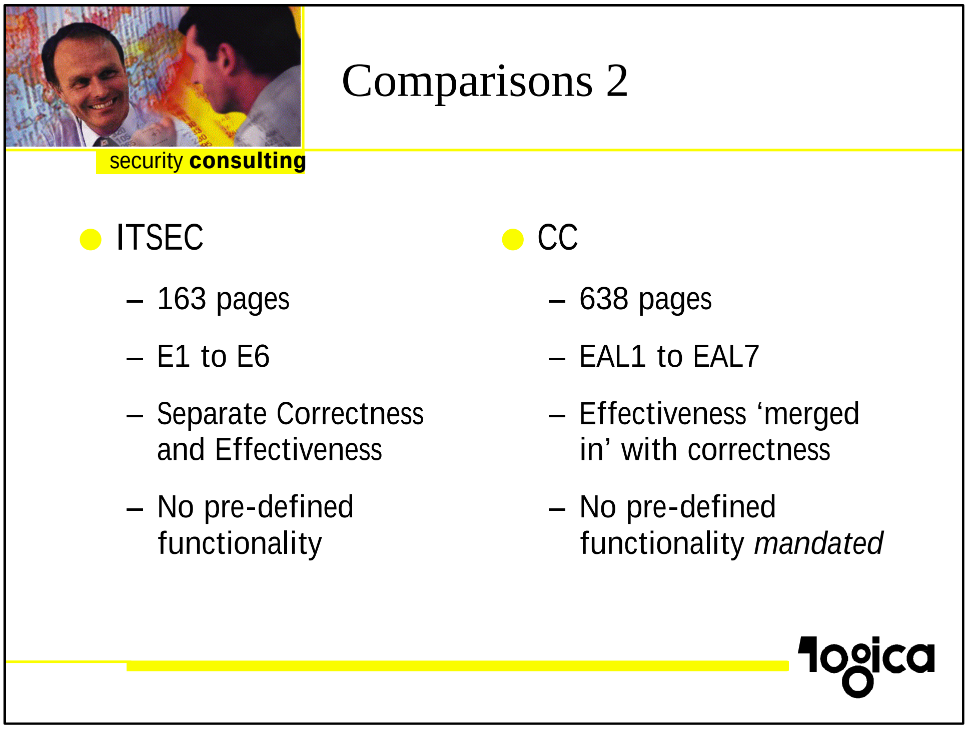
The right hand side highlights the “European approach” where everything is more generalised.

The American approach may be seen as more objective (since there are more things defined, there is less scope for variation). The European approach may be seen as more subjective, since in every case it is necessary to derive most of the things that are already specified in the America approach. However, the European approach is more flexible, allowing faster innovation and, for example, evaluation of networked systems and smartcards.

Each approach as its advantages and its drawbacks.

The Canadian criteria (CTCPEC) had adopted an approach in the middle ground of specifying things in more detail than the ITSEC and yet still allowing flexibility.

This was subsequently built upon by the CC. In particular, Part 3 (assurance) draws heavily on the ITSEC, while Part 2 draws heavily on the Orange Book.



Comparisons 2

security **consulting**

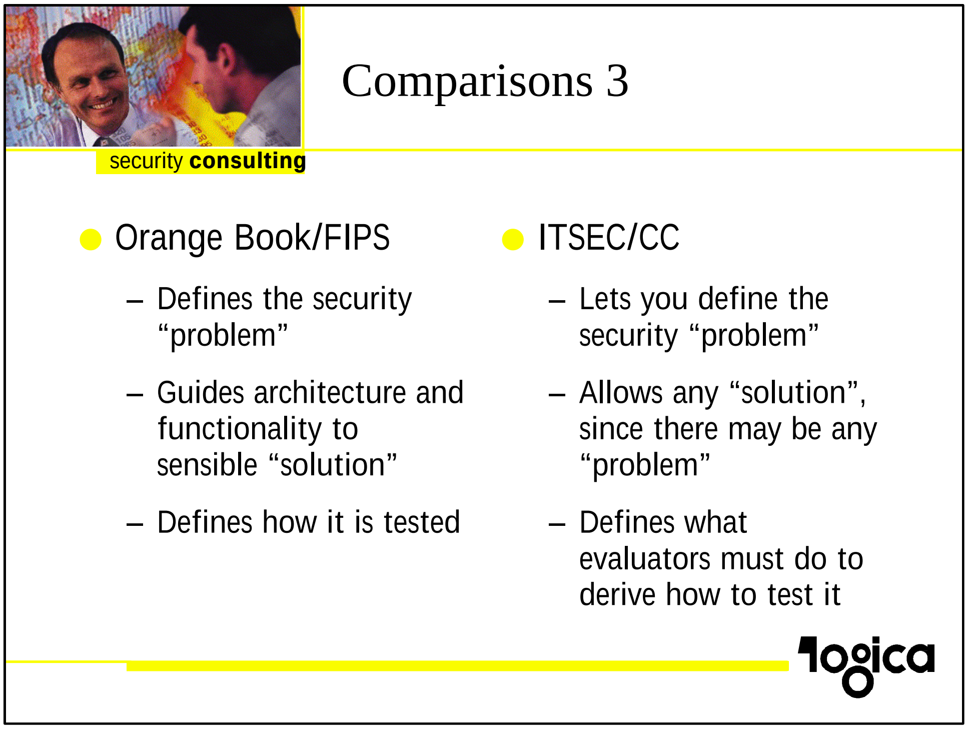
- ITSEC
  - 163 pages
  - E1 to E6
  - Separate Correctness and Effectiveness
  - No pre-defined functionality
- CC
  - 638 pages
  - EAL1 to EAL7
  - Effectiveness ‘merged in’ with correctness
  - No pre-defined functionality *mandated*

logica

The Common Criteria is much much bigger than the ITSEC was. The CC has more flexibility (in terms of being able to define assurance levels). It also has Part 2 on functionality, which is almost entirely new from ITSEC. The CC generally has more detail in it to help to avoid misunderstandings. The ITSEC in turn was bigger than most of its ancestors.

The CC introduces a new low assurance level (EAL1) below E1.

The ITSEC concept of effectiveness was not well understood. The ITSEC wanted to make sure that the effectiveness aspects were covered, and hence enumerated then as separate requirements. The perception of developers and to some extent evaluators was that documents are required. This is not the case, the ITSEC only calls for information; not documents.



Comparisons 3

security **consulting**

- Orange Book/FIPS
  - Defines the security "problem"
  - Guides architecture and functionality to sensible "solution"
  - Defines how it is tested
- ITSEC/CC
  - Lets you define the security "problem"
  - Allows any "solution", since there may be any "problem"
  - Defines what evaluators must do to derive how to test it

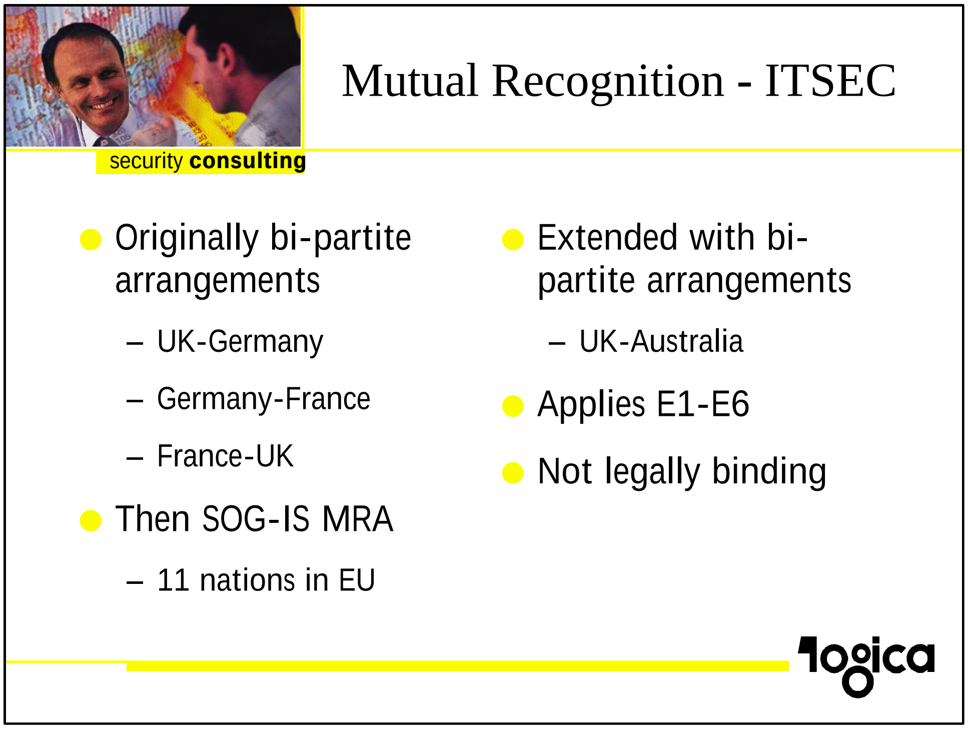
logica

To those used to the Orange Book and FIPS 140, the ITSEC and the CC will look similar and strange. Rest assured that to those familiar with the ITSEC, the CC looks a bit like the Orange Book, and yet also strange.

The ability to select different assurance levels for the same functionality is new to those familiar with the OB. It presents a problem of answering the question "What is the right level of assurance?" - a question that didn't need answering before. It also can present the question "What functionality do I need for a given assurance?". Again this is a new question.

To those familiar with the ITSEC, there is a new challenge of expressing functionality in a constrained and artificial way. It is necessary to 'translate' into this common language rather than to express freely.

It is likely that people familiar with the ITSEC will accommodate to the relative constraints of the CC more easily than those familiar with the constraints of the OB will accommodate to the freedom of the relative CC.



security **consulting**

Mutual Recognition - ITSEC

- Originally bi-partite arrangements
  - UK-Germany
  - Germany-France
  - France-UK
- Then SOG-IS MRA
  - 11 nations in EU
- Extended with bi-partite arrangements
  - UK-Australia
- Applies E1-E6
- Not legally binding

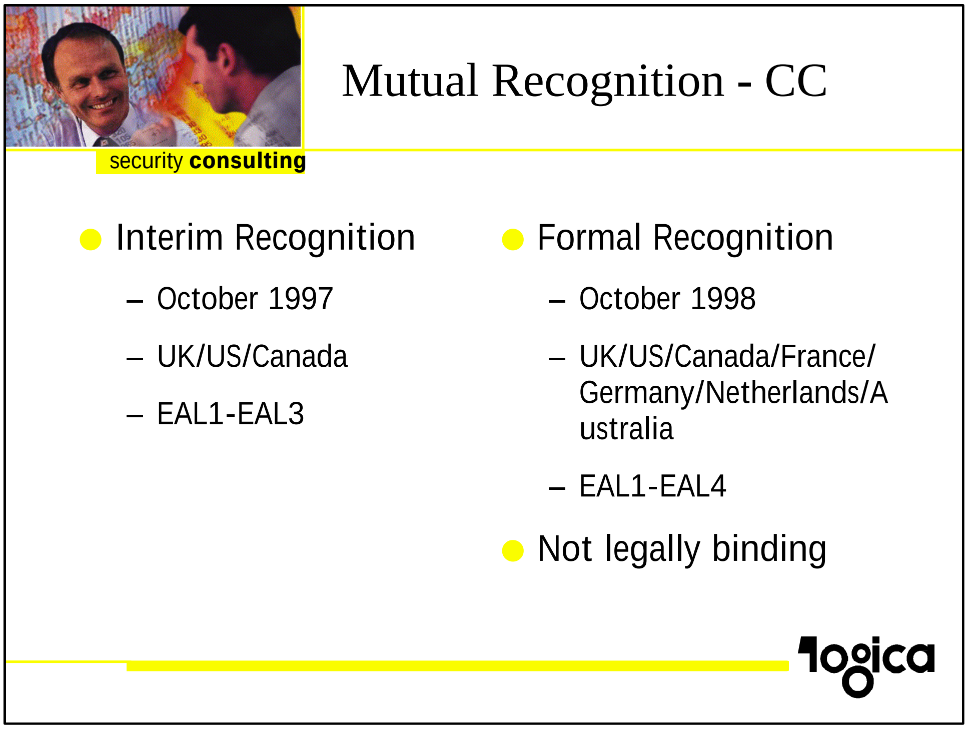
Although it is relatively easy to decide at a technical level that two nations are working to broadly the same technical standards (if not always to the same method) and achieve equivalent results, it is much harder to say that the results will *a priori* be accepted.

Prior to any formal mutual recognition, there were various informal understandings. These varied from accepting results on a case-by-case basis (possibly following technical discussions or review of the technical work) to the broader policy of “It is better if it has been evaluated somewhere than if it has not been evaluated at all”. This was, of course, caveated by national pride (or rather a better understanding of own processes and procedures) saying “It is best if we have evaluated it”.

Bi-partite arrangements are OK when there is a small community. As the community grows, it is necessary to use more general agreements and a system that defines how the membership can change. This is what we now have for the Common Criteria.

Note that none of the agreements is legally binding - it is more of a gentleman’s agreement. Also note that there is an exclusion clause that allows nations to decline recognition of a certificate where nationally sensitive information is to be protected by a product.

The ITSEC agreement has wider scope at present - both in terms of number of members and assurance levels covered. However, American dominance of the IT market makes a CC certificate valuable.



security consulting
logica

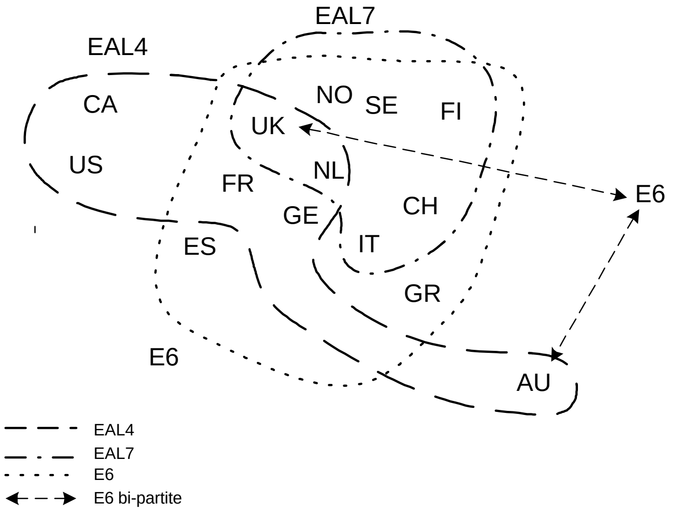
Mutual Recognition - CC

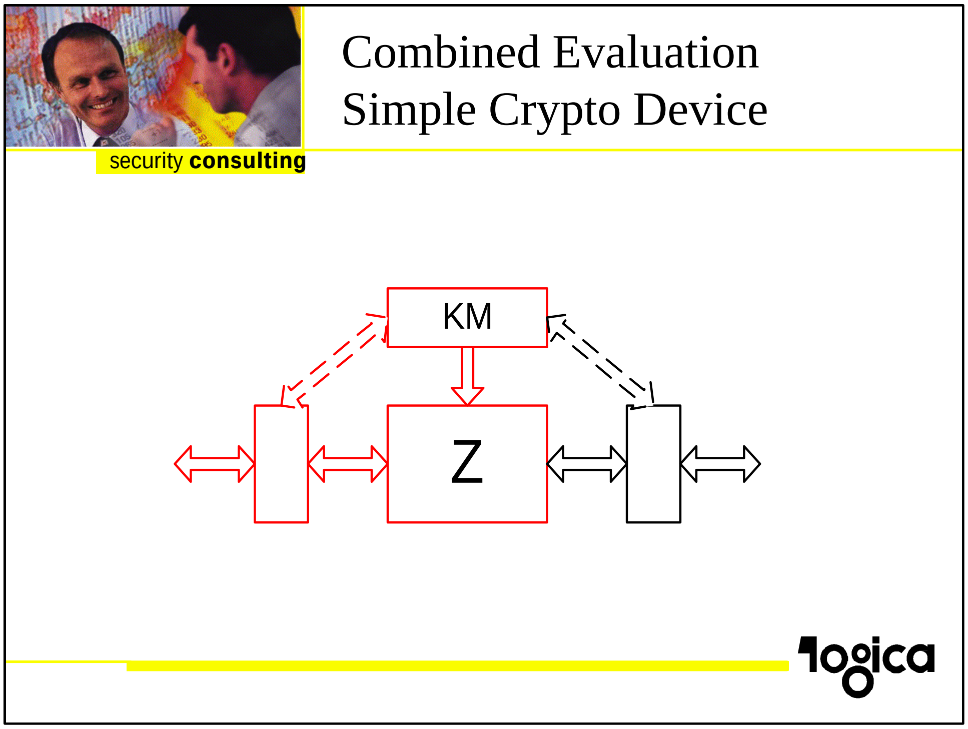
- Interim Recognition
  - October 1997
  - UK/US/Canada
  - EAL1-EAL3
- Formal Recognition
  - October 1998
  - UK/US/Canada/France/ Germany/Netherlands/A ustralia
  - EAL1-EAL4
- Not legally binding

The group of 6 has mutual recognition to EAL4. This was recently extended to include Australia (announced at the 22nd NISSC conference in October 1999).

In addition, there is recognition to EAL7 currently amongst Finland, Italy, Norway, Sweden, Switzerland, Netherlands and the UK as an extension of the SOG-IS agreement. There are moves to bring CC-MRA and SOG-IS under the same umbrella.

In all cases, there is an exclusion clause for national security. Therefore, in some cases, a certificate in one country is not necessarily enough for recognition in co-signatory countries.





security **consulting**

Combined Evaluation Simple Crypto Device

logica

Now for some of the practicalities and challenges of using evaluation and assessment schemes.

A ‘simple’ crypto device can easily be represented by 4 components. There is an input and an output interface, the encryption module and a key management module. The Key Management is likely to have an external interface for key loading and selection. There may also be interfaces to allow selection/rotation of keys from one or both interfaces.

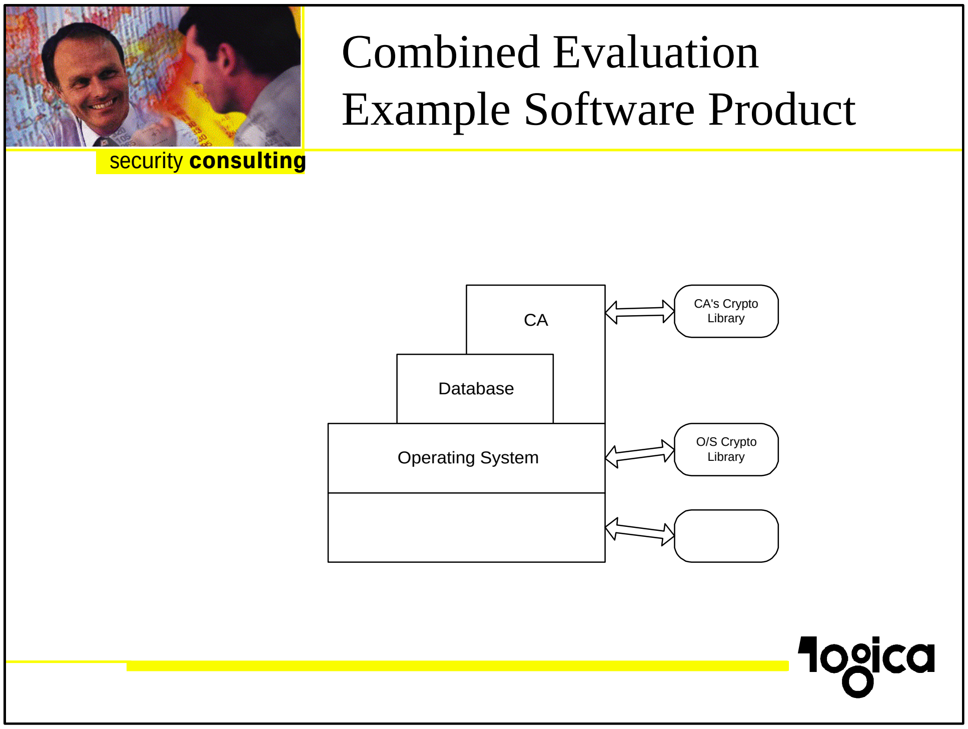
There will also often be a crypto bypass and overall management function.

Portions dealing with cleartext are RED and cypertext are BLACK. Good crypto design will keep red and black separate.

This design is (relatively) easy to implement in hardware and it appears to be the model used in FIPS 140.

Real crypto systems are rarely this simple. Many cheaper commercial systems will not employ internal separation to the degree of the above model due to cost constraints. For example, a commercial crypto may use a single microprocessor to manage all functions (e.g. KM, red and black interfaces) and may use unsegregated memory for buffers. Greater assurance can be provided by using multiple microprocessors, separate memory *etc*.

In the UK - for government use - it is common for the crypto engine and crypto bypass to be assessed by CESG (the nearest equivalent to FIPS 140) and for all the remainder to be evaluated under the ITSEC/CC. Following a recent policy change, the CESG process is now open to certain “public domain” algorithms through a combination of CAPS and the UK ITSEC Scheme.



security **consulting**

Combined Evaluation Example Software Product

CA

Database

Operating System

CA's Crypto Library

O/S Crypto Library

The simple model works well for simple devices, especially devices that are dedicated to providing encryption and only encryption.

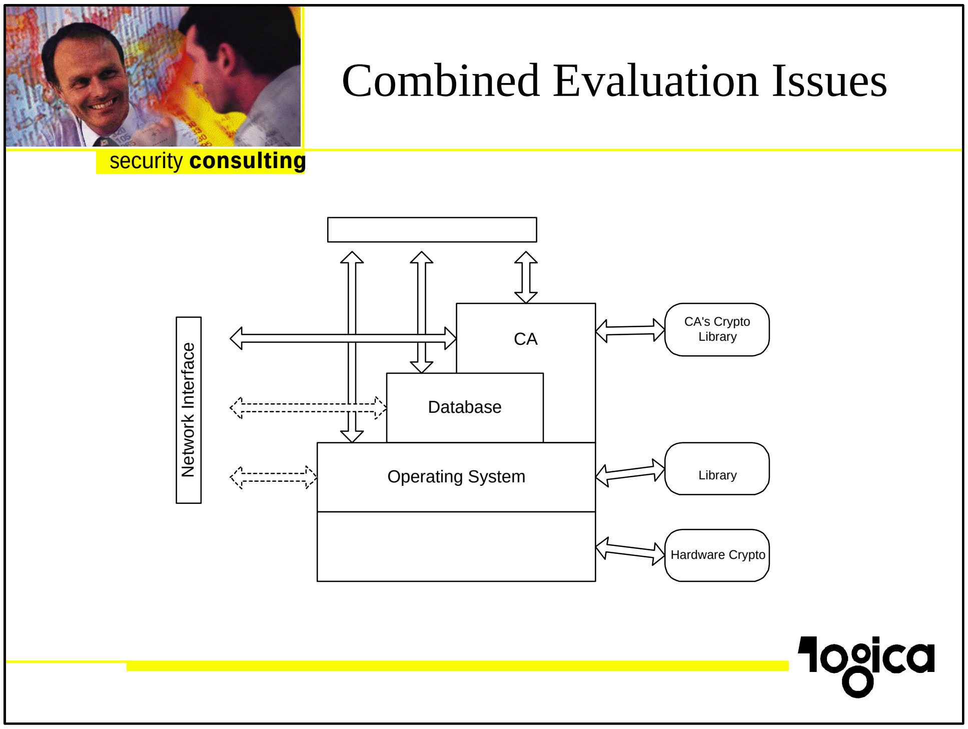
In practice there are very few devices that match the simple model. Things that do match it are bulk or line encryptors That are applied to insecure comms channels. This is classical Government use of encryption.

Encryption is now widely used as a small (but important) part of diverse functionality. The security of the whole depends on security at every stage. On the Internet/Intranet technologies, systems are vulnerable to interception and tampering of data in transit between machines.

As well as application level encryption, there is Operating System level services (*e.g.* Microsoft’s CryptoAPI). There is also emerging hardware crypto built into systems (most notably IBM’s motherboard crypto for PC 300PL and IntelliStation, and to a lesser extent 3Com’s EtherLink 10/100 with 3XP). In addition, there may be a hardware security module provided for the CA for crypto acceleration and key generation.

In the case of using a CA’s Crypto Library, it is easier to see how an ITSEC/CC evaluation and a FIPS 140 assessment can “join up”. In any other case, it is far less clear, especially since there may be user interfaces to the same resources (can a user’s actions detect/affect randomness?).

Note that the assumed environment for a CA is likely to be much stricter than is assumed for a database or operating system evaluation in terms of user access, and much more lax in terms of network access.



security **consulting**

Combined Evaluation Issues

It is likely that an evaluation of a database will not include accessing the database over a network. Although an evaluation of an operating system may include some form of networking, it is very likely to be limited to a homogeneous network, and also be in a single administrative domain.

However the database and operating system evaluations will have expected local user access.

Most CA's will want connections to public networks like the Internet. The network aspect of the CA may have been included in the evaluation of a CA. However it is likely to have assumed that everything else was OK. So, unless some effort is directed at issues such as:

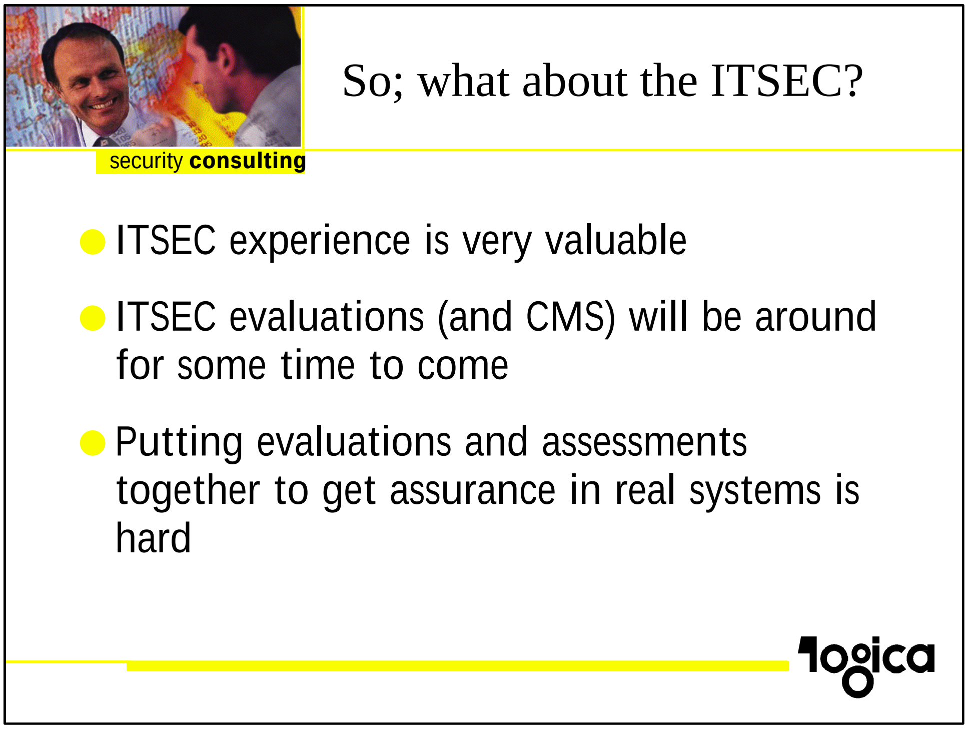
• Can the database be accessed over the network by untrusted parties?

• Can the operating system be accessed over the network by untrusted parties?

• Can attacks be launched over the network which would affect operation of the CA (e.g. Ping of Death, SYN flooding, ...)

• Can any 'other effects' affect the CA; for example can network operations adversely affect the entropy pool (either for CA's own library or a shard one)

Producing a really useful evaluation, mixing evaluation of components, and evaluation to other criteria is still a big challenge.



security **consulting**

So; what about the ITSEC?

- ITSEC experience is very valuable
- ITSEC evaluations (and CMS) will be around for some time to come
- Putting evaluations and assessments together to get assurance in real systems is hard

Experience in the ITSEC is not wasted by a move to the CC. Many of the concepts in the CC are drawn from the ITSEC or are based on a common philosophy. This also applies to the Orange Book - the philosophy is similar, but the way that the CC expresses and expects to attain assurance is very different. Developers and evaluators have transferable skills.

For various reasons, ITSEC evaluations will continue into the future. On the introduction of the ITSEC in the UK, there was a 2 year transition to the ITSEC. This turned out to be too short for developers, even when there were relatively few evaluations being performed. For the CC there is no planned cut-off at present - the UK is taking a “wait and see what the market requires” approach. Developers that are committed to the Certificate Maintenance Scheme are likely to to move over to the CC through “top-up” evaluations and then full-blown evaluations to coincide with their engineering/marketing plans.

At present, to obtain maximum possible coverage of mutual recognition of certificates, it is necessary to perform an ITSEC evaluation and a CC (top-up) evaluation. The greatest possible scope for mutual recognition is on the basis of certificates issued in the UK.