



CESG

Developing a Methodology for Biometric Security Testing

Nigel Gordon

nigel.gordon@cesg.gsi.gov.uk

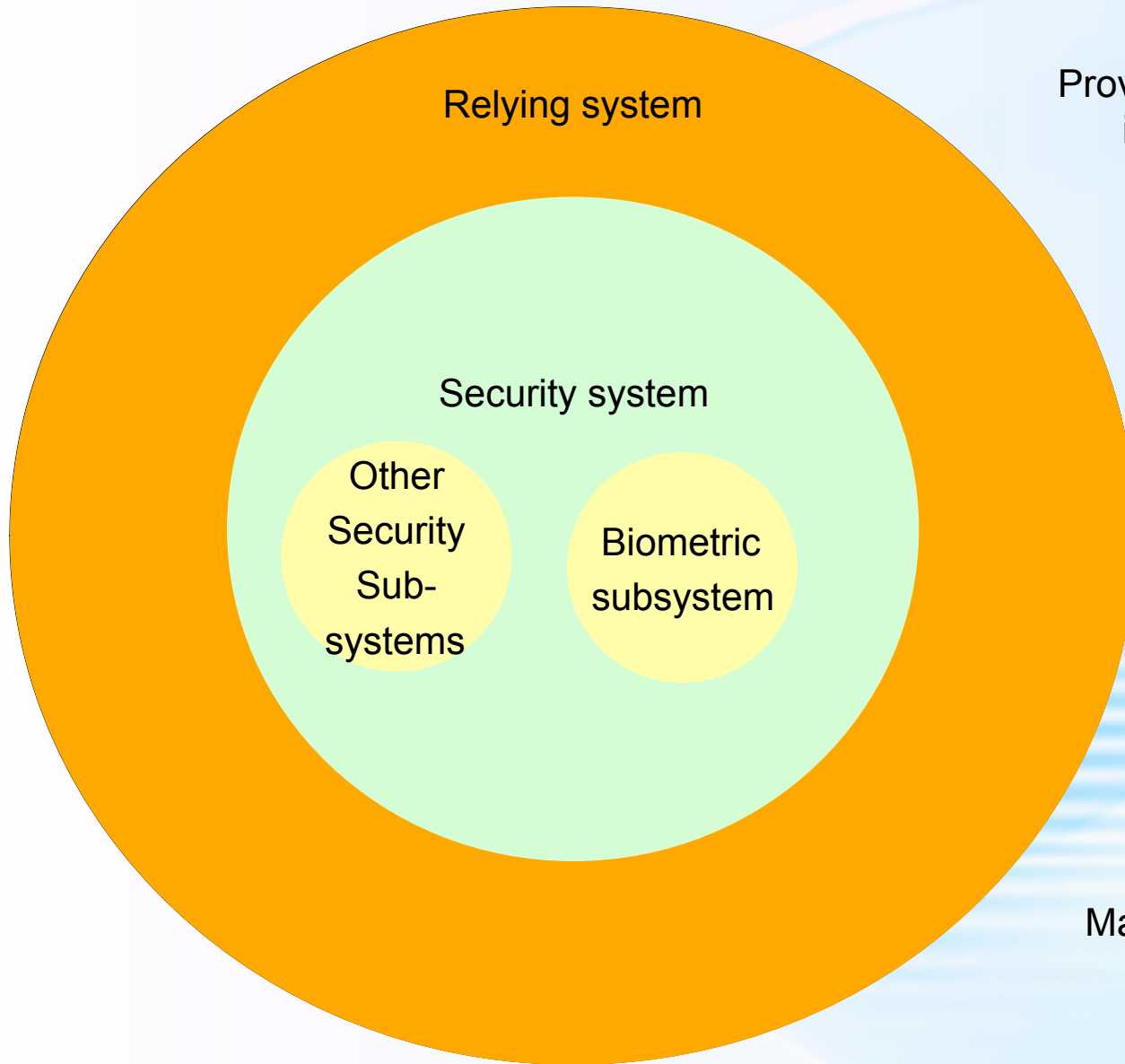
Aims of Testing

- To evaluate a system against a requirement specification
- To identify vulnerabilities
- For contractual compliance
- To rank candidate systems
- To check claims by suppliers

What needs to be tested?

- Ability of system to reject imposters
- Ability of system to match an enrolled user
 - Construction of artefacts
 - Testing of artefact detection

But this is only a small part of the story!



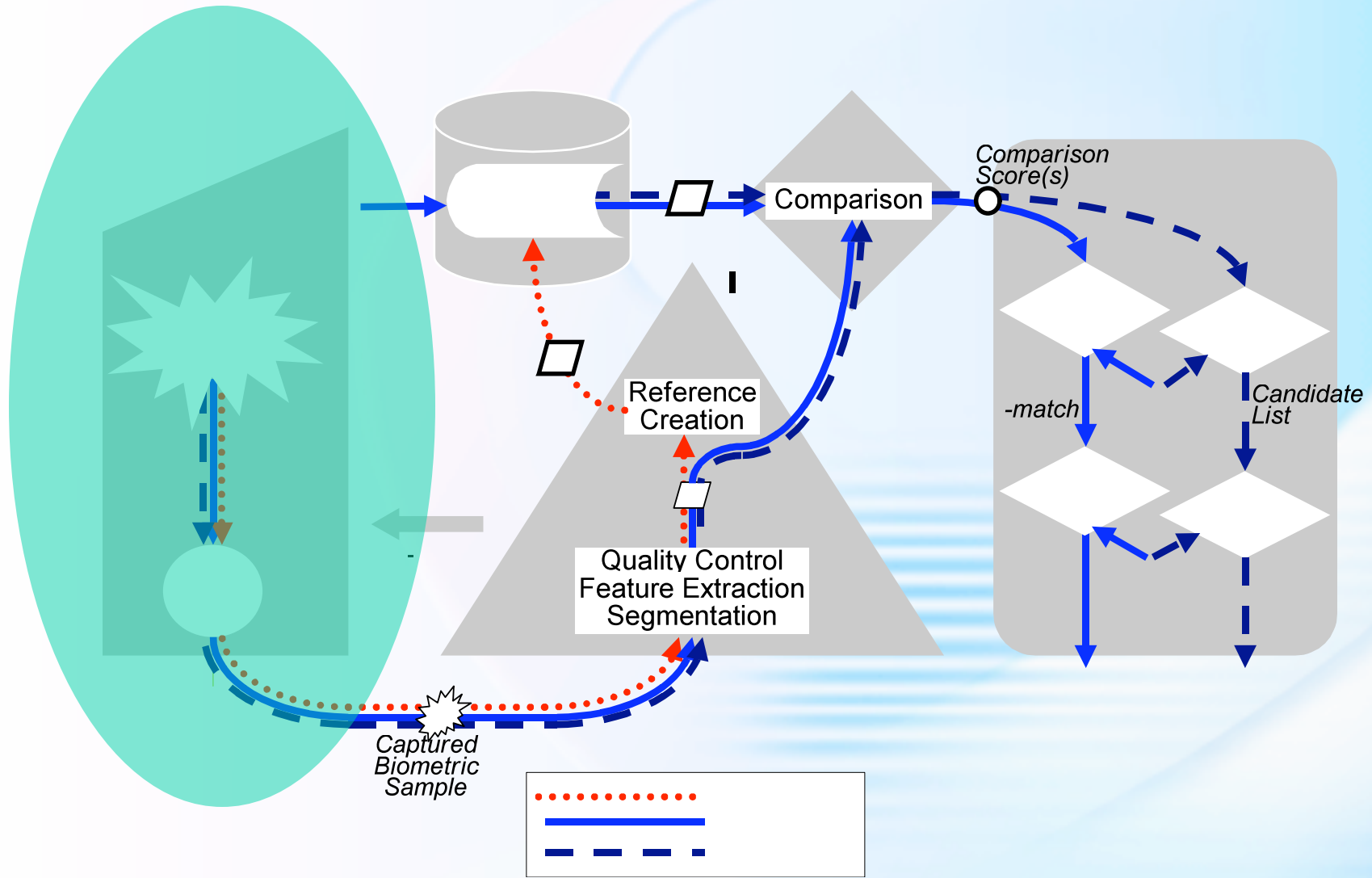
Provides recognition of individuals

Makes business decisions and performs functions based on output of security system

- Biometric subsystem provides some security functionality
 - Which elements does it provide?
 - Which elements are unique?
 - How good do they need to be?
 - How do they relate to the security requirement
 - How do we trade them off against others or against factors such as usability?

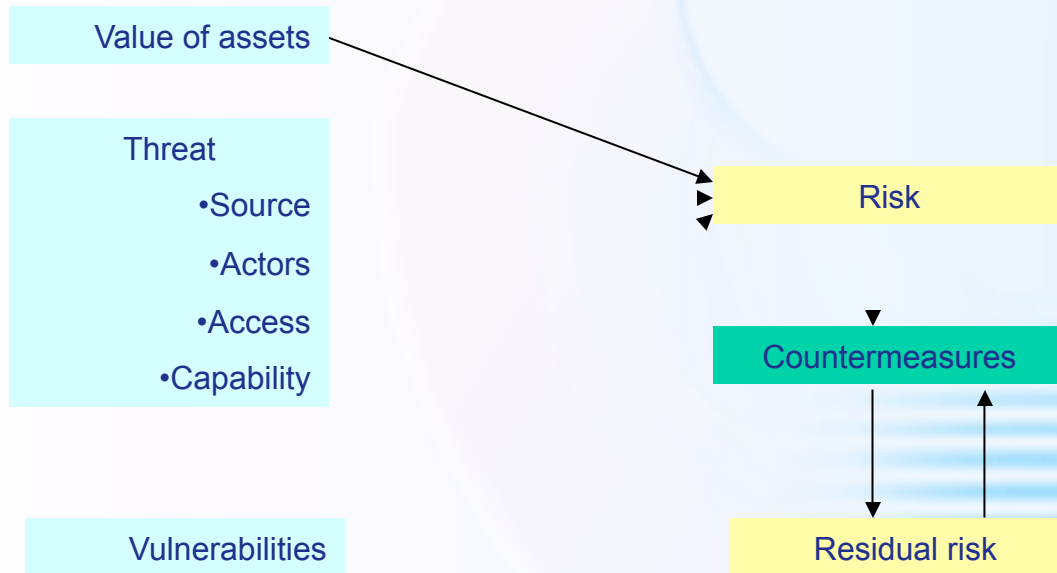
What does security mean in a biometric system?

- Biometric functionality provides security enforcing functions
- Spoof-resistance/liveness detection and other countermeasures provide protection against malicious users
- Biometric systems are IT systems with all of their inherent vulnerabilities
- The use of biometric data introduces its own security or privacy requirements



- Overall security involves much more than testing and protecting the integrity of the biometric sensor
- Cannot assess biometric security in isolation
- A methodology is required
 - Based on existing techniques (preferably integrated)
 - Generic – usable with a range of assurance approaches
 - Needs to provide a bridge between biometrics and IT (and other) security

All modern IT security assurance methodologies are based on risk management



Testing is required to find vulnerabilities, quantify the risk and verify the effectiveness of countermeasures

Existing methodologies

- Most countries have methodologies of this type (IAS1 in the U.K.)
- There are also multinational and international methodologies
- None of them addresses biometrics in any detail

CESG Methodology

- Provides a structure and context for testing and evaluation
 - Demands that the assets are identified and the threat is understood
 - Forces an understanding of how countermeasures address vulnerabilities
 - Requires a mapping of security requirements to biometric performance parameters (ISO TR29156)
- Allows us to combine and trade-off biometrics and other ‘security enforcing functions’

CESG Methodology (2)

- Requires a (semi) quantitative assessment of vulnerabilities and countermeasures
 - For higher assurance levels these will need to be verified by testing
- Currently ‘work in progress’.
 - First part addresses top level issues
 - Provides a link between biometrics and IT security
 - Will be followed by modality-specific annexes
 - Should make use of work from other agencies where appropriate and possible

Points to consider

- How quantitative should we aim to be?
- Vocabulary – what does false non-match mean when the data subject is using an artefact?
- How meaningful is a lab test – how do we model the training of operators etc?
- Need much more (and more accurate) information about countermeasures from suppliers
- Aim for balanced security – but things change

Points to consider (2)

- Continuum of 'environmental' factors (including user behaviour) that can affect performance from benign users, through difficult populations to hostile attackers
 - Where do factors such as using make-up, cosmetic surgery, ageing, injury etc. fit on the scale?
- Is there a need for standardisation?
 - SC 37/27?
- Remember procedural security and the all-important fallback system



Questions

nigel.gordon@cesg.gsi.gov.uk