A. Problem Statement
Existing proxy based authentication approaches have problems (e.g., non-binding, susceptible to theft and dictionary attack, burden on end-users, re-use risk). Biometrics, which authenticates users by intrinsic biological traits, arises to address the drawbacks. However, the biometrics is irreplaceable once compromised and leak sensitive information about the human user behind it.

B. Technical Rational, New Model and Approach
We propose a simple yet effective mechanism “Biometric Capsule”. The proposed mechanism fuses biometrics of a user and a (physical) Reference Subject and extracts BC for authentication.

New requirements for Biometrics:
• Diversity: do not allow cross matching across databases.
• Revocability (Cancelability): compromised template is revocable.
• Security: hard to obtain the original biometrics from secured template.
• Performance: not be degraded compared to conventional system.

B. Technical Rational, New Model and Approach

No additional user requirements for using BC (as some existing approaches does): training, additional PINs
No need for error-correct code, helper data, and no key length limitation

Preliminary Result and comparisons:

C. Features and Potential Applications

(a) Provably secure (b) Usable and identity-bearing: a biometric-binding identity, plus non-intrusive continuous authentication, provides traceability and mitigate liability. (c) Privacy preserving (d) Biometric cancelable (e) General applicable: working with existing biometric modules. (f) Interoperable: supports “one-click sign on” across multiple systems by using a distinct RS on each system. (g) Cost-effective and easy to use: transparent to end-users, no user training.

User-centric identity ecosystem: the new BC based model is promising in developing a highly resilient, privacy-preserving, revocable, interoperable, and efficient user-centric identity verification and protection ecosystem.

Active authentication system: the new BC based approach is encouraging in developing a provably secure, privacy-preserving, biometric active authentication system to support continuous and non-intrusive authentication.