CERIAS

the center for education and research in information assurance and security

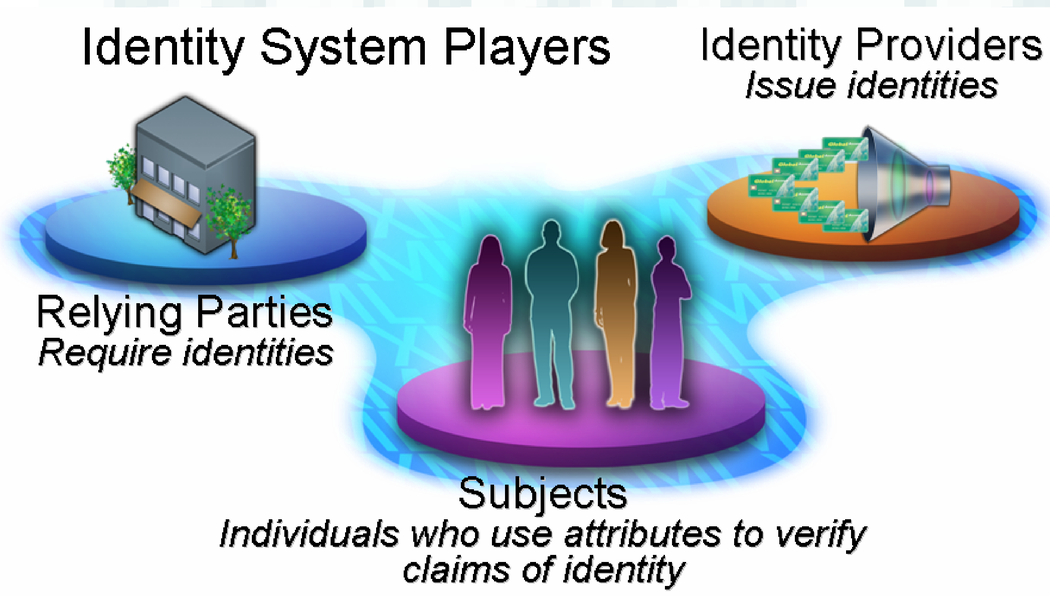
Bio-Key : Privacy Preserving Biometric Authentication

E. Bertino[1], S. Elliott[2], A.Bhargav-Spantzel[1], M. Young[2], S. Modi[2],A. Squicciarini[1]

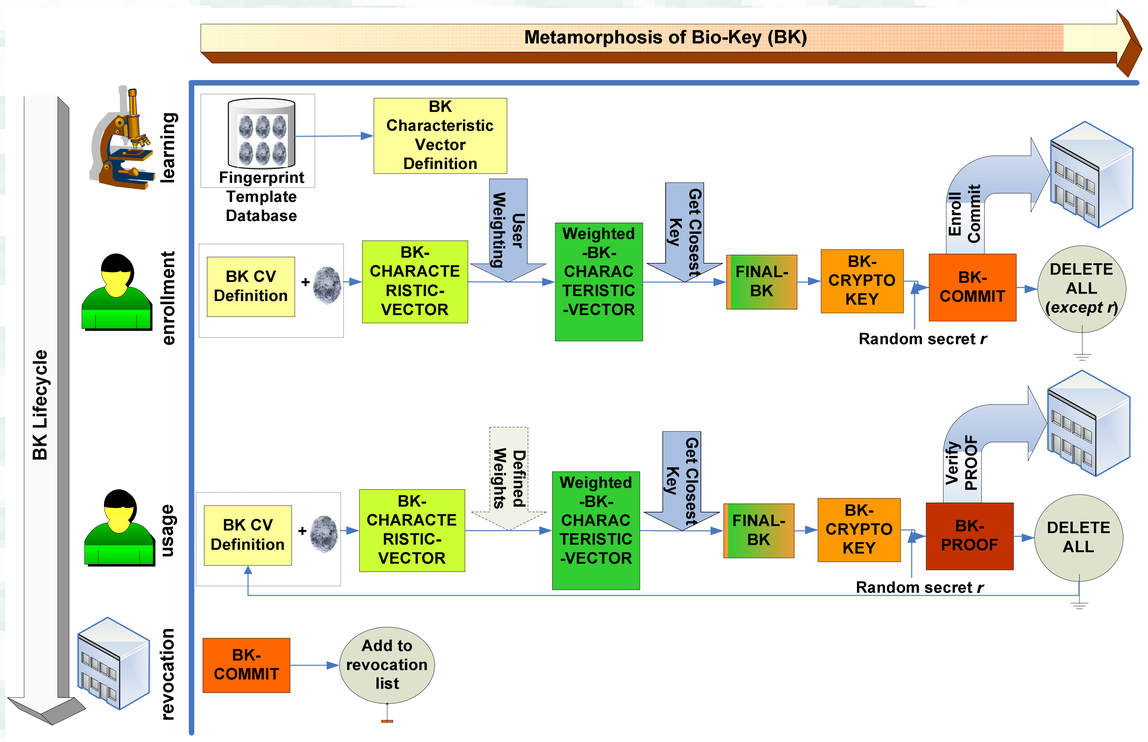
[1]Department of Computer Science, [2]Department of Industrial Technology. Purdue University

Goals & Advantages:

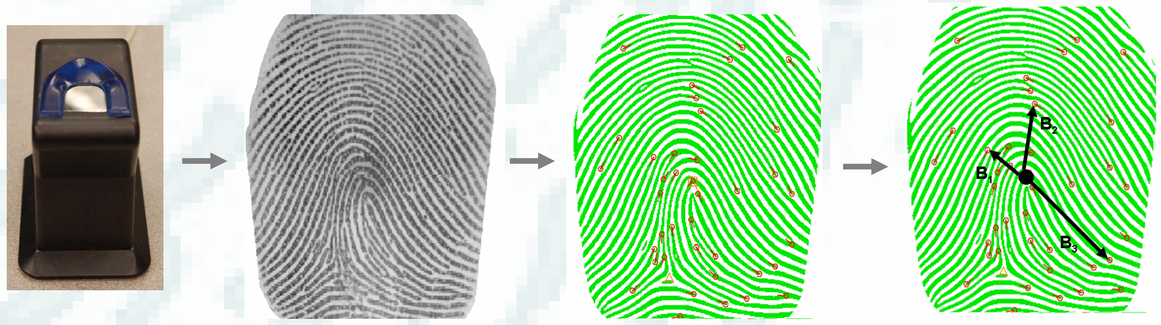
- **The goal** is to *provide a privacy preserving methodology* for strong biometric authentication in federated identity management systems.
- Privacy Preserving Multifactor Authentication [1]: multifactor authentication is essential for secure authentication mechanisms. The identity management framework is used to provide proofs of multiple strong identifiers for a given user.
- Interoperability: Our scheme provides an interoperable, usable, secure, and inexpensive to use biometric authentication in a federation.
- User Control : The raw biometric never leaves the client machine therefore providing complete control to its owner.



Bio-Key Lifecycle:



Bio-Key Transformation:



- Sensor / Raw Image / Feature Extraction / Vector Creation

ID Attributes:

Alice@Registrar1 | *PARAMS*

Strong IdTag	Commit-ment [M]	assurance	WeakID (list)
CCN	32983979798722 3493827983	good	Value: Alice, tag: fname, assure: B; Value: Mars, tag: lname, assure: B
SSN	39872398747923 2738294991	undecided	Value: Alice, tag: fname, assure: A; Value: 12442, tag: zip, assure: B
FINGERPRINT	72987466621004 7937477211	good	Value: Cap-bio, tag: sensor, assure: A; Value: 80, tag: threshold, assure: A

Collaboration Through CERIAS:

- Department of Computer Science
- Biometric Standards, Performance & Assurance (BSPA) Laboratory (Department of Industrial Technology)

Reference:

[1] A. B. Spantzel, A. C. Squicciarini, E. Bertino. ***Establishing and Protecting Digital Identity in Federation System***. In proceedings of ACM CCS workshop on Digital Identity Management .

PURDUE UNIVERSITY

CERIAS

Discovery Park e-Enterprise Center