CONTRIBUTION FROM TRANSACTION SECURITY, INC. FOR THE USE OF BIOMETRICS AND CRYPTOGRAPHY IN MOBILE DEVICE SECURITY
An amended version of a paper originally prepared in May, 2013

BIOMETRIC PASSWORD GENERATOR
PASSWORD OBFUSCATION/DE-OBFUSCATION/ENCRYPTION PROCESS

5% of mobile devices are lost or stolen each year. Therefore there can be little certainty that characters entered into the device are being entered by the owner or by the authorized user. The object of this process is to provide a very high level of assurance that transactions carried out on the device are those of the owner/authorized user. In addition we protect the DAR, including the on-board local biometric template, from exposure through strong encryption. We accomplish this by obfuscating and storing complex Passwords so that they can later be de-obfuscated and released to authenticate transactions of all kinds and encrypt appropriate data. This also relieves the user from the need to remember and enter complex passwords for device unlock, for single sign-on and for network authentication.

An early prototype of some of this methodology using the UUID as the hardware root was implemented some time ago on a Windows Mobile Device using the Crypto-Sign® (www.crypto-sign.com) signature/sign biometric modality, which uses, as the biometric sample, a secret sign submitted on the device with inking inhibited. A similar methodology can be used with any biometric modality where an appropriate sensor is available on the device.

A prototype was demonstrated at the Mobility for Defense event in Crystal City in December, 2012. The user-friendly combination of the secret sign and an entered PIN meets FIPS 140/2 level 3 authentication requirements limiting the probability of access by chance to less than one in a million and, we believe, makes a successful brute force attack extremely difficult because of the need to submit a biometric sample (as well as a PIN) for every attempt.

The Crypto-Sign method uses a stylus or a finger to generate the biometric sample and provides for a very low-cost solution. The behavioral nature of the Crypto-Sign biometric technology means that, in the unlikely event of compromise, a new sign can easily be re enrolled. The complex password can be changed easily at any time without having to remember and enter the old one.

If this biometric procedure were executed in an on-board ASIC, full hardware-rooted encryption (as opposed to using the device UUID) and consistent software behavior would also be achieved.

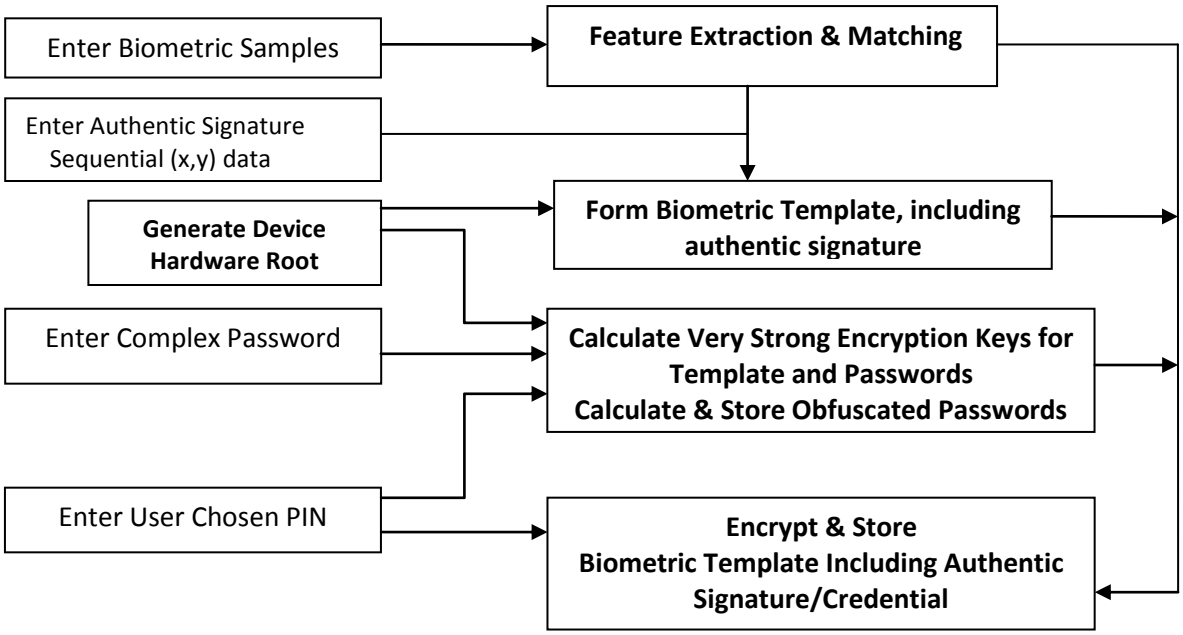
Rod Beatson
Transaction Security, Inc.
Rod.Beatson@crypto-sign.com
919-533-6762

Jan 27, 2015

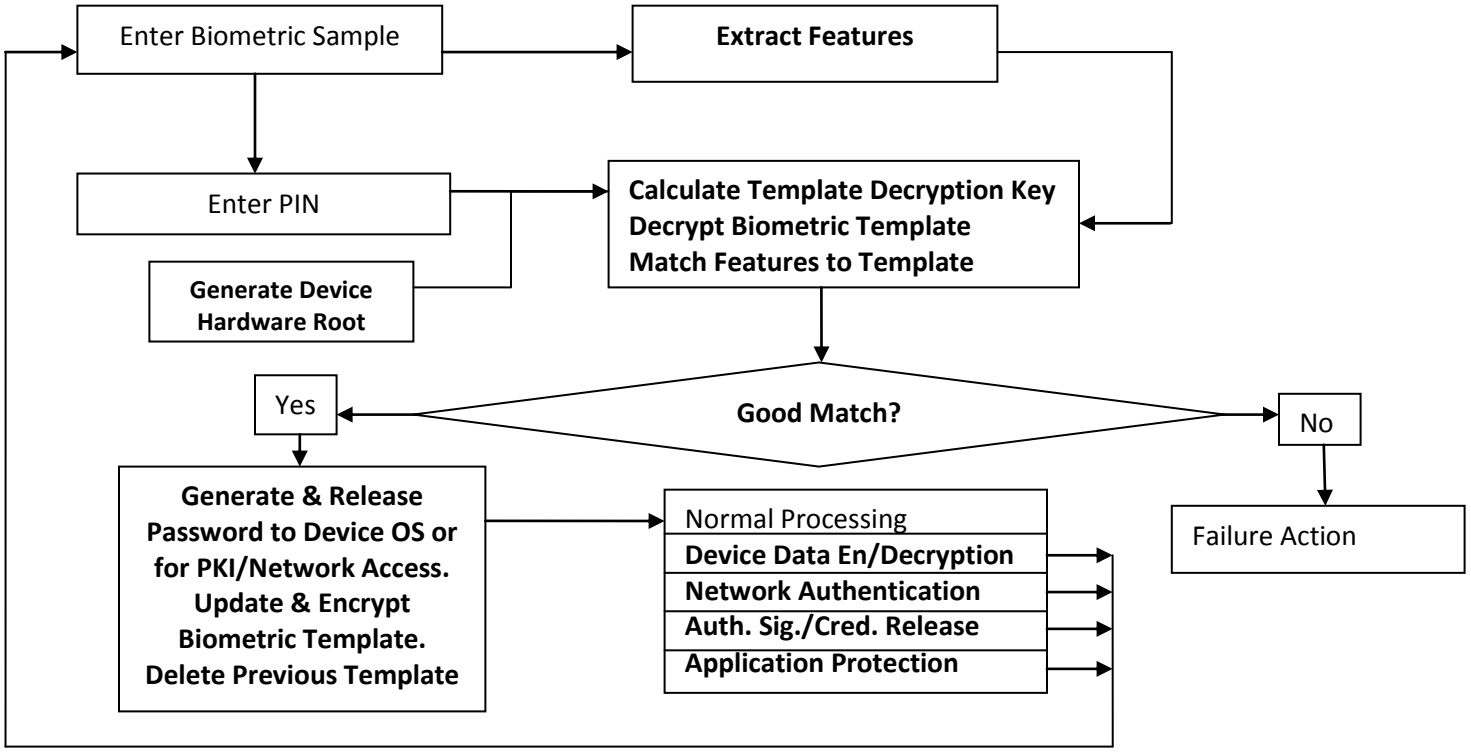
CONTRIBUTION FROM TRANSACTION SECURITY, INC. FOR THE USE OF BIOMETRICS AND CRYPTOGRAPHY IN MOBILE DEVICE SECURITY
An amended version of a paper originally prepared in May, 2013

A Biometric Password Generator - Operational Schematic

1) REGISTRATION & ENROLLMENT - Covering the use of general biometric technologies for password generation and transaction security



2) AUTHENTICATION AND PASSWORD GENERATION/RELEASE



CONTRIBUTION FROM TRANSACTION SECURITY, INC. FOR THE USE OF BIOMETRICS AND CRYPTOGRAPHY IN MOBILE DEVICE SECURITY
An amended version of a paper originally prepared in May, 2013

1) **REGISTRATION & ENROLLMENT** - This sets the process up for seamless operation during **the** authentication process. The functionality here is to:

a) Collect a consistent set of biometric samples that can be used to form the biometric template (signature/sign or other modality) and form the initial template. Various in-built tests are conducted on the data to ensure consistency and a sufficient level of complexity
b) Choose and enter a quality authentic electronic signature, with an ink-on paper look (or some other credential) that may be used later to submit to a relying party. Several attempts may be required and the user should be prompted to accept or re-sign after each attempt until a quality authentic signature is attained. This signature will be the one released to future signature-bearing transactions – e.g. healthcare/financial transactions. The format is a set of sequential (x,y) data, which are stored with the template in encrypted form. It is possible for styli that provide a pressure value to use this to provide variations in the thickness of the stroke but the process should not rely on these data being available.
c) A value, rooted in the chip hardware is then calculated
d) Choose and enter complex passwords (enterprise or user/process defined) that meet certain minimum standards of complexity.
e) A user-chosen PIN is then entered.
f) These external data, suitably transformed are then used to:
    i. Calculate a very strong encryption key for the biometric template
    ii. Calculate (and store in NV storage) obfuscated passwords
    iii. Encrypt and store the biometric template
    iv. Protect sensitive device data at rest

2) **AUTHENTICATION – No entry of complex Password required.**

The authentication process uses a biometric sample from the user together with PIN entry as follows:

a) Capture the biometric sample and PIN
b) Calculate the biometric template decryption key
c) Decrypt the biometric template and match it to the (features extracted from) the biometric sample
d) De-obfuscate the password
e) Responsive to a good match, release the password to the device authentication system, or for encryption purposes.

3) **OTHER FUNCTIONALITY**

The same process can be used to:

a) Encrypt and protect sensitive device data at rest
b) Release passwords for Network access and/or for the SSL
c) Protect access to sensitive device applications.
d) Provide a trusted signature, with an ink on paper look (or other personal credentials) for financial transactions and other credential-based transactions e.g. in Healthcare, Financial Transactions and for Contractual Agreements.

3) PASSWORD OBFUSCATION/DE-OBFUSCATION/ENCRYPTION MODEL - Brief Description

We will assume:

UBS – is a user biometric sample
BT – is the clear text biometric template created from biometric samples.
TEK – is the biometric template encryption/decryption key.
f – is a symmetric encryption function as e.g. in the AES
f^{-1} – is the symmetric decryption function as in the AES
EBT – is the encrypted biometric template
CPW1 - is a complex password for device unlock
CPW2 – is a complex password for Network Access or for the SSL.
Different passwords for different purposes might be defined in this manner and can be changed by the user without having to enter the old password
HWR – is a unique device number rooted in the device hardware.
PIN – is a user-chosen PIN
PIN# - is a one-way hash of the PIN
OPW1 – is the obfuscated password for device unlock
OPW2 – is the obfuscated password for network access/PKI.
DAR - is sensitive device data at rest.

Then we define:

OPW1 = f(CPW1,HWR,PIN#)
OPW2 = f(CPW2,HWR,PIN#)
TEK = f(OPW1,HWR,PIN#) - encrypted value of OPW1 using a key derived from HWR and PIN#
EBT = f(BT,TEK) - encrypted value of BT using TEK as the key
BT = f^{-1}(EBT,TEK) – decryption function for biometric template using the TEK key.

We can now compare the features extracted from the biometric sample with the biometric template (BT) and if all is well, update the template, delete the old template, re-encrypt and store the new one and use the de-obfuscated password, CPW1, in the device authentication process.

OPW1 and OPW2 are de-obfuscated by:

CPW1 = f^{-1}(OPW1,HWR,PIN#) where f^{-1} is the symmetrical decryption of OPW1 using the same key combination of HWR and PIN# as was used to encrypt CPW1

CPW2 = f^{-1}(OPW2,HWR,PIN#) may then be used for Network access and/or as a single sign-on to various passwords used in the SSL.

DAR may be encrypted/decrypted using a key derived from CPW1 according to NIST SP 800-132 or it may use TEK.