Trusted BWI: Privacy and Trust Enhanced Biometric Web Identities

Abdullah A. Albahdal, Hamdan Alzahrani, Lalit Prithviraj Jain, and Terrance E. Boult
University of Colorado at Colorado Springs
Colorado Springs, CO 80918
{aalbahda, halzahra, ljain2, tboult }@uccs.edu

Abstract

Trusted web identities, which strongly associate a person with a digital identifier or certificate, are an area where biometrics should play a critical role. Balancing usability, security, and privacy is an important issue for any system that captures/stores users' information, especially for any biometric-based technology. To support biometric web services, the Biometric Identity Assurance Services (BIAS) standard was developed and recently approved. BIAS aims to establish standard biometric web services in order to improve interoperability and platform independence. Because they involve biometric data, the deployment of BIAS (and biometric web services in general) faces many challenges in terms of privacy, trust and security. They also face compatibility issues with widely-deployed systems that combine biometric sensors and Trusted Platform Modules (TPM). In order to address these obstacles, we propose an enhanced design of the recently introduced Biocryptographic Key Infrastructure (BKI). The original BKI enhanced the privacy and trust of remote biometric transactions, but, like most existing biometric systems, ignores the trust issues associated with remote enrollment. Our enhanced BKI design addresses this problem of trusted remote biometric enrollment. In addition, the enhanced design also extends the BKI to support biometric sensors with cryptographically secured on-chip biometric matching. Leveraging the new enhanced version of BKI, we propose the Trusted Biometric Web Identities (Trusted-BWI), as privacy and trust-enhanced biometric web services.

1 Introduction and Background

Responding to the increasing demand for biometric web services, the InterNational Committee for Information Technology Standards (INCITS) and the American National Standards Institute (ANSI) have approved the Biometric Identity Assurance Services (BIAS) standard [1]. BIAS was issued as a result of collaboration between different organizations from the public and private sectors. BIAS provides a standard definition for biometric web services, with the goal to enhance interoperability and allow platform and language independent remote access of biometric web services and sensors. The Organization for the Advancement of Structured Information Standards (OASIS) BIAS profile [4] complements BIAS standard by defining the binding of BIAS to the Simple Object Access Protocol (SOAP) in order to implement BIAS web services.

As biometric web services deal with Personally Identifiable Information (PII), biometric web services should pay attention to the security/privacy of users' biometric and biographic data. Moreover, special attention should be paid to securing users' biometric data since, if it is compromised, it cannot be revoked or replaced, reducing its potential for strong authentication purposes. BIAS leaves securing biometric and biographic data to BIAS implementers. Unfortunately, the BIAS reference implementation [5] lacks security and does not respect the privacy aspect of users' biometric data. BIAS reference implementation sends users' fingerprint images in clear from the BIAS client to BIAS service! Even if a secure transport protocol is used (i.e. Secure Socket Layer (SSL)), as recommended by OASIS BIAS profile [4], users' biometric data is still not secure while stored or processed. Moreover, reliance on users' raw or easily invertible biometric data, even for trusted services, is still a security and privacy risk.

Alternatively, privacy-enhanced biometric techniques could be used for applications that do not require the original biometric data (i.e. legal or governmental high secure applications). Jain et al. [8] surveys multiple biometric template protection techniques. Such privacy-enhanced techniques might be leveraged for enhancing the privacy of biometric web services, but it requires extensions to most existing approaches to make them suitable for remote web-based usage.

Besides the privacy issue, BIAS (and remote biometric transactions in general) faces a trust challenge. For instance, even though a user has authenticated himself/herself successfully to a biometric web service, should this remote user be trusted for enrolling himself/herself? What about if the user spoofs someone else's biometrics in this remote unsupervised enrollment? The severity of this problem becomes higher with applications that have a high level of security such as governmental, financial, and medical applications. Even though there are many existing standards for securing biometrics systems (i.e. the ISO/IEC standard for the biometric information protection [2]), none of these standards address the trust issue for the remote biometric enrollment. In programs such as the US Personal Identity Verification (PIV) of Federal Employees and Contractors [3], the identity proofing and biometric collection process is detailed, extensive, and invasive. Many citizens would not subject themselves to such an invasive process. However, without some level of trusted enrollment, the resulting web identities are weak.

In addition to the privacy and trust issues, BIAS, like many other biometric systems, does not support the new generation of security and privacy-enhanced biometric sensors that combine trusted modules and sensors to perform biometric matching on-chip without disclosing users' biometric signal. BIAS requires a representation of biometric data, hence BIAS cannot not support users with these types of privacy-enhanced sensors. Examples of these types of biometric sensors include [6] [12]. Such privacy-enhanced biometric sensors are widely deployed on laptops and mobile devices. For example, Authentec[1] claimed shipping over 100 million of these sensors before their acquisition by Apple. These sensors combine secure storage and cryptographic hardware. In these types of secure biometric sensors, the matching is performed on the sensor, and, if the matching is successful, the biometric sensor releases the user's credential or signs/decrypts using the user's private key that is stored on the sensor's secure storage. With the Apple acquisition of Authentec, one of the largest manufacturer of biometric sensors and the owner of the sensor of [6], we expect that this type of biometric sensing technology will continue to grow in popularity in the near future.

In this paper, we aim to address the aforementioned issues of trusted web identities, BIAS, and biometric web services in general. These issues include enhancing the privacy and trust of biometric web services and solving compatibility issues with biometric sensors that have cryptographically-secured on-chip biometric matching. To achieve these objectives, we introduce two elements. First, we introduce a new and improved design of Biocryptographic Key Infrastructure (BKI) [13]. This enhanced design of BKI aims primarily to enhance the trust of remote biometric transactions by enhancing enrollment processing and by supporting secure on-chip matching biometric sensors. Secondly, we leverage the new developed BKI to propose the Trusted Biometric Web Identities (Trusted-BWI) as privacy and trust enhanced biometric web services. Trusted-BWI is designed with built-in support for biometric sensors with cryptographically secure on-chip matching. Figure 1 illustrates an overview of Trusted-BWI services.

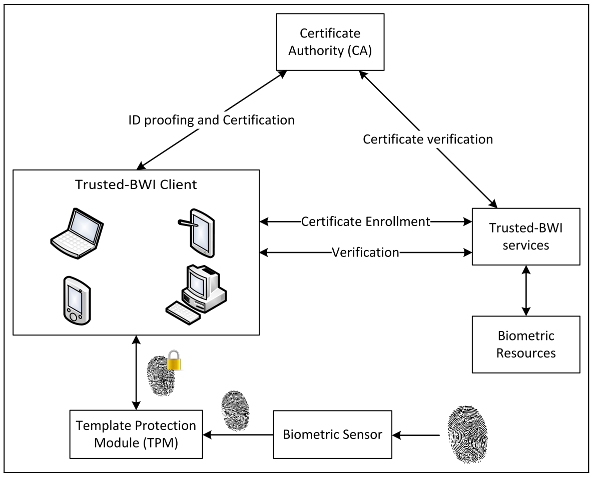

Figure 1. Overview of Trusted-BWI web services. An extended BKI uses a Template Protection Module (either software or hardware) which produces a Public Key/Private key and protects the private key, requiring biometric matching to use it. The CA does identity proofing with it, represented in the resulting certificate. The certificate can be enrolled in a Trusted-BWI server and used for later verification. The model allows trusting CAs for identity proofing; however, the Trusted BWI servers may also have their own CA. Privacy is maintained since traditional biometric data is not used outside the Template Protection Module. Stronger binding of digital certificates to identity, in a scalable manner, with privacy enhanced remote/client side matching, makes Trusted-BWI ideal for web-based applications needing trusted identities.

Contributions of this paper can be summarized as follows. 1) We develop an improved version of BKI to enhance the trust of remote biometric transactions with improved enrollment and built-in support for biometric sensors with cryptographically secure on-chip matching. 2) We propose Trusted-BWI as an approach for privacy and trust enhanced biometric web identities.

2 Biocryptographic Key Infrastructure (BKI)

Public Key Infrastructure (PKI) has been used to enhance the trust of public key exchange, which is otherwise vulnerable to man-in-the-middle attacks. However, PKI has its weaknesses because users are not strongly bound to their cryptographic keys, so users cannot really establish their identities by relying only on these cryptographic keys. For example, when Alice signs a message using her private key, Bob cannot say that Alice has signed the message herself. Instead, Bob only knows that Alice's private key was used for signing, not that Alice personally signed the message. This is because that keys can be shared or stolen, then used without the owners' knowledge. Scheirer et al [13] introduced the BKI in order to overcome the aforementioned problem of PKI. Before the BKI was proposed, there were many pro-

[1] http://www.authentec.com/

posals to integrate biometrics into X.509 certificates such as [9] [7] [11]. Unlike these proposals, BKI is the only solution that respects the privacy of biometric data. In addition, prior work combining biometrics with certificates, including the original BKI, does not address the critical issue of how certificates represent the trust in the certification process.

To enhance the trust and privacy of BKI, we introduce a new improved design BKI framework. Our motivations for improving the BKI are as follows. Firstly, BKI should be leveraged to enhance the trust of remote biometric transactions. It follows that a biometric certificate should identify the level of trust for biometric data attached to the biometric certificate. For example, a Certificate Authority (CA) can accept remote certification of users' biometric and authentication documents or require in-person authentication of biometric data for certification. The biometric certificate itself should reflect the level of identity proofing that the CA has used for certification. Secondly, BKI does not support the widely deployed biometric sensors with cryptographically secure on-chip matching, which perform secure on-chip matching and do not disclose users' biometric data. This discrepancy leads to our motivation to find a solution that enables the use of these types of biometric sensors without reducing the security of BKI framework. The rest of this section describes our enhanced design and implementation of BKI framework.

2.1 Certification and Identity Proofing

The user initiates the certification process by creating a Certificate Signing Request (CSR). CSR, as shown in Figure 2, contains the user's general information, public key, and one or more biometric extensions (i.e. for multiple biometric modalities or positions). Each biometric extension consists of the biotoken type (i.e. biometric technology and modality used), a biotoken, and a biometric public key. The CSR is signed with the private key corresponding to the biometric public key attached to the CSR. The signed CSR is then sent to the CA for certification.

Each biometric extension will contain a biotoken and/or a biometric public key. We use the term *biotoken* to refer, in a technology neutral manner, to the biometric data that results from a secure and compatible key-binding biometric template protection scheme. In order to be compatible with BKI, the key-binding biometric template protection scheme must support both binding a key with a biometric template and releasing the key after a successful matching. Example of a secure and compatible template protection scheme is the Bipartite Biotoken [14]. Table 1 shows the matching accuracy of the Bipartite Biotoken with different key sizes.

We introduce the concept of an *Asymmetric Bio-Cryptographic Subsystem (ABCS)*, which uses the *biometric public key*. The ABCS is a subsystem, ideally in firmware or hardware, that provides asymmetric cryptographic operations (e.g. public key encryption) with biometric authentication necessary to access or use the *biometric private key*. The biometric private key is intended to be used or accessed only after biometrically authenticating the key's owner. To achieve this goal, we propose four approaches with different levels of security. Firstly, the biometric private key could be kept inside a secure hardware trusted processor module, i.e., in hardware tightly bound with the biometric sensor and only used by the sensor's cryptographic processor to sign or decrypt upon successful biometric matching. Secondly, with a lower level of security, the biometric private key could be encrypted with a key that is kept inside the trusted biometric sensor and only released upon successful biometric matching. Thirdly, there is growing movement toward Virtual TPM [10] and Firmware Trusted Platform Modules (FTPM)[15], reducing cost and addressing issues of trusted hardware in various countries while providing a "Trusted Execution Environment (TEE)", and either of the first models could use any TEE. Finally, a software model is the alternative to securing the biometric private key. The software model embeds the biometric private key into a biotoken, or embeds a key that encrypts the biometric private key into a biotoken. The biometric private key, or its decryption key, is only released from the biotoken when matched against the legitimate user's biometrics. Ideally the software or firmware for the ABCS would be separate from the operating system. Introducing ABCS allows BKI to enhance the level of authenticity for using the biometric private key and allows BKI to support biometric sensors with cryptographically secure on-chip matching.

Key-binding Template Protection Scheme	FAR	GAR
Bipartite Biotoken 128-bit key	0	97
Bipartite Biotoken 256-bit key	0	97
Bipartite Biotoken 1024-bit key	0	82

Table 1. Comparison of matching accuracy (False Accept Rate (FAR) vs. Genuine Accept Rate (GAR)) of the Bipartite Biotoken scheme with different key sizes.

In order to enhance the trust of biometric certificates, CA should define its policy for identity proofing of users during the certification process. For example, a CA can authenticate users' documents, biometrics, or both. Also, the CA can certify users remotely or request users to present in person for authentication. Moreover, the CA could require users to bring in their secure biometric sensors that support on-chip secure cryptographic matching in order to authenticate that the biometric private key is bound to the biometric sensor hardware. In addition, the biometric data (i.e. biotoken or biometric public key) attached to a biometric certificate can be authenticated remotely, relying on a challenge-and-response authentication protocols. In this manner, the biometric certificate should reflect how the identity proofing of the certified user has been done. This information helps other entities to determine the trustworthiness of a biometric

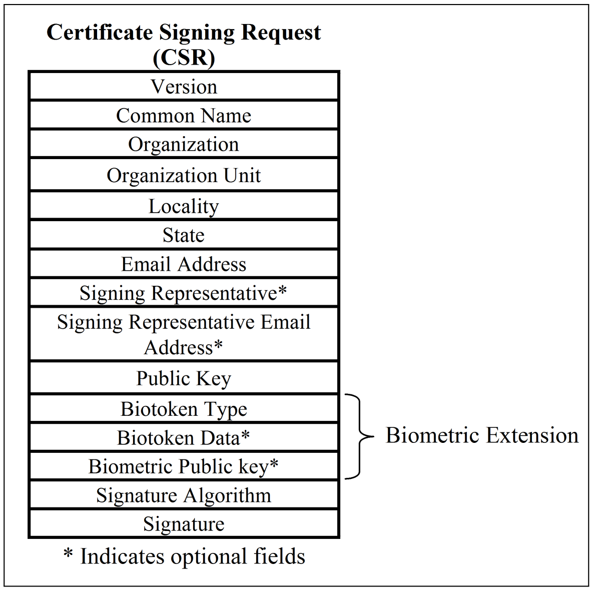

Figure 2. Format of Certificate Signing Request (CSR).

$$\underbrace{DD}_{\text{CA biometric auth. level}} \quad . \quad \underbrace{DD}_{\text{CA documents auth. level}} \quad . \quad \underbrace{DDDD}_{\text{CA reissue auth. level}}$$

Figure 3. Format of the CA Identity proofing level field.

certificate. Figure 3 illustrates the format of the CA identity proofing level field. The CA identity proofing level field consists of three numbers that represent the CA biometric authentication level, document authentication level, and reissue authentication level respectively. Table 2 defines the different CA biometric and documents authentication levels to be used for the CA identity proofing level field in the biometric certificate, including gaps intentionally left for future refinements of levels, e.g. treating driver's license different than passports for documents. The reissue authentication level is discussed in detail in section 2.2.

Besides requiring the user to present in person for certification (i.e. which is not always a practical solution), the CA can remotely authenticate the user biometrics using the biometric extension attached to the CSR. For a CSR attached with a biotoken, the remote biometric authentication can be performed using a challenge-and-response authentication protocol, such as the two way authentication protocol proposed by Scheirer et al [13]. For a CSR attached with a biometric public key, the CA can remotely authenticate the user using a remote biometric authentication protocol that relies on the BKI's ABCS. (i.e. ABCS with a secure biometric sensor with a hardware trusted module). An example of this authentication protocol is presented in section 2.3. A sensor of these types of biometric sensors could have its own digital certificate that is signed by a trusted CA (i.e. the manufacturer of the biometric sensor). The biometric public key, in turn, could be signed by the secure biometric sensor in order to indicate that its corresponding biometric private key is kept inside the sensor's secure hardware and is only used by the sensor's cryptographic processor, never leaving the sensor. For any third party, such as the CA certifying a CSR with a biometric public key, it can verify that the biometric private key is kept inside the secure sensor by verifying the sensor's signature on the biometric public key after verifying the sensor's digital certificate.

No.	CA biometric authentication levels
00	No biometric authentication is used.
10	CA remotely authenticates the user's biotoken using a remote authentication protocol.
20	CA remotely authenticates the user's biometric public key using a remote authentication protocol.
30	CA authenticates, in person, the user's soft biotoken and biometric public key (i.e. using a local challenge and response protocol).
40	CA authenticates, in person, the user's TEE with biometric public key (i.e. by requiring the user to bring in the device with TEE).
50	CA authenticates, in person, the user's hardware biometric public key (i.e. by requiring the user to bring in the secure biometric sensor with hardware trusted module).
No.	CA documents authentication levels
00	No document authentication is used.
10	CA authenticates remotely the user's documents.
20	CA authenticates, in person, the user's documents.

Table 2. CA biometric and documents authentication levels.

After authenticating the user, the CA can certify the user by signing the user's certificate using the CA private key. Figure 4 shows the format of the biometric certificate. Besides the fields included in the CSR and traditional X509 certificate, the biometric certificate includes the CA Identity proofing extension. The CA Identity proofing extension defines how the CA has performed the identity proofing for the certified user. Moreover, the CA Identity proofing extension can include the CA signing representative's ID and his/her signature on the user's authentication documents. The CA Identity proofing extension can be used in case of a dispute to prove which CA signing representative has authenticated the user based on the signed documents, with the potential non-repudiation deterring insiders from inappropriate actions. The CA can store users' authentication documents in an encrypted format which can later be used for revalidation or security inspection.

2.2 Revocation and Reissuance

In many cases, a CA is required to revoke issued biometric certificates for any number of reasons. For example, a CA can revoke a biometric certificate when the user's private key, the CA's private key, the user's biotoken, or the ABCS sub-

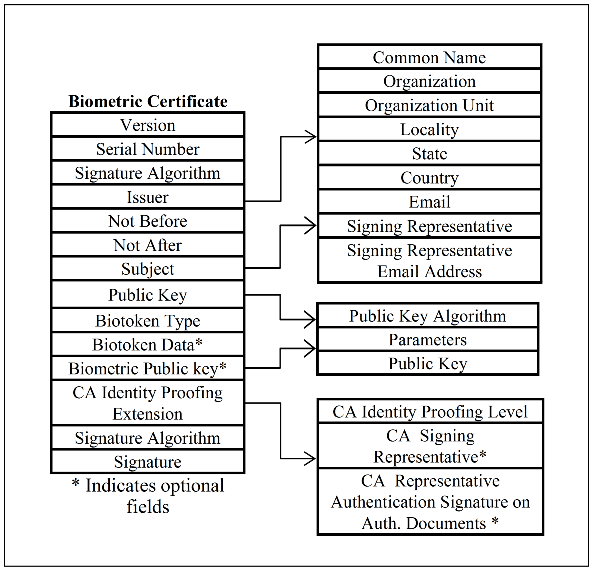

Figure 4. Format of biometric certificate.

system are compromised. Accordingly, the CA can reissue the user's biometric certificate with new identity proofing requirements. For example, when the user's private key is compromised, the CA is not required to perform any identity proofing for the user's biometrics at reissuance time. For any third party, knowing how the CA has performed the identity proofing for a reissued biometric certificate helps to determine the trustworthiness associated with a biometric certificate.

The CA identity proofing extension addresses the trust issue for reissued biometric certificates. In particular, The last four digits of the CA identity proofing level field contain the CA reissue authentication level, which articulates how the CA has performed the identity proofing for reissuance. The first two digits indicate the CA biometric authentication level while the last two digits indicate the CA document authentication level for the reissued certificate. The reissue authentication level is set to 0 (i.e. one digit instead of four) if the biometric certificate is not a reissue.

2.3 Authentication Protocols

The biometric certificate has capabilities that can be leveraged to develop remote biometric authentication protocols. Scheirer et al [13] describe two- and three-way remote biometric authentication protocols using biotokens attached to users' biometric certificates. Similarly, the BKI's ABCS subsystem (i.e. biometric public and private keys) can be used for developing remote biometric authentication protocols. Figure 5 illustrates the remote biometric authentication protocol using BKI's ABCS subsystem.

Alice and Bob participate in this remote biometric authentication protocol in order to authenticate each other (i.e. mutual strong authentication). This remote biometric authentication protocol leverages the capabilities provided by

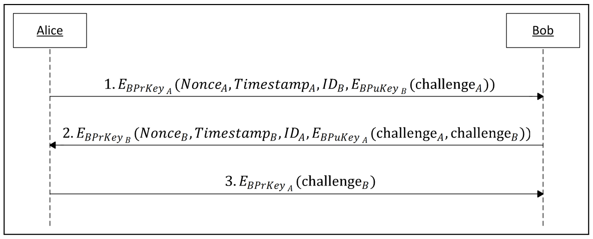
Alice
Bob
1. $E_{BPrKey\,A}(Nonce_A, Timestamp_A, ID_B, E_{BPuKey\,B}(\text{challenge}_A))$
2. $E_{BPrKey\,B}(Nonce_B, Timestamp_B, ID_A, E_{BPuKey\,A}(\text{challenge}_A, \text{challenge}_B))$
3. $E_{BPrKey\,A}(\text{challenge}_B)$

Figure 5. The remote authentication protocol using biometric public and private keys.

biometric certificates. Also, to enhance the level of trust, this authentication protocol relies on ABCS cryptographic processing, allowing it to use a secure biometric sensor with a trusted cryptographic module. The ABCS secures the biometric private key and only uses it for encryption or decryption upon successful biometric matching. Hence, each usage of the biometric private key in this authentication protocol comes after biometric authentication of the user by the ABCS. Also, the biometric public key is included in a biometric certificate that is signed by a trusted CA, which also enhances the level of trust since the CA has verified that the biometric private key is tightly bound with designed ABCS – including labeling the level of protection (hardware/firmware/software). We will now describe our proposed remote biometric authentication protocol using the biometric public and private keys.

1. Alice starts the protocol by sending Bob a message signed with her biometric private key. The signed message consists of a nonce created by Alice $Nonce_A$, a timestamp created by Alice $Timestamp_A$, the identity of Bob ID_B, and a cryptographic challenge created by Alice and encrypted with Bob's biometric public key $E_{BPuKey_B}(challenge_A)$. Upon receiving Alice's first message, Bob verifies the message's signature and checks that the timestamp $Timestamp_A$ is fresh and that the nonce $Nonce_A$ has not been already used. Then Bob extracts Alice's challenge by decrypting it using his biometric private key (after biometrically authenticating himself to the ABCS in order to use his biometric private key for decryption).
2. Bob replies with a message signed with his biometric private key. The reply message consists of a nonce created by Bob $Nonce_B$, a timestamp created by Bob $Timestamp_B$, the identity of Alice ID_A, and Alice's recovered challenge $challenge_A$ with a new cryptographic challenge created by Bob $challenge_B$. Both are encrypted with Alice's biometric public key $E_{BPuKey_A}(challenge_A, challenge_B)$. Upon receiving Bob's message, Alice verifies the message's signature and checks that the timestamp $Timestamp_B$ is fresh and that the nonce $Nonce_B$ has not been already used. Then Alice extracts Bob's challenge $challenge_B$ and Bob's response to her challenge $challenge_A$ by decrypting both

challenges using her biometric private key.

3. If Alice sent challenge $challenge_A$ and Bob's response to her challenge $challenge'_A$ matches, Alice sends Bob's challenge $challenge_B$ back to Bob signed with her biometric private key. Bob receives Alice's message and checks its signature. Then Bob checks if Alice's response to his challenge $challenge'_B$ matches his sent challenge $challenge_B$. If both challenges match, the authentication protocol ends, and both parties have biometrically authenticated each other.

2.4 Implementation

For implementing the new enhanced BKI, we leveraged the X.509 certificate implementation of OpenSSL Crypto library. This allows current systems that use X.509 certificates to handle biometric certificates with minimum modifications. Moreover, our implementation of biometric certificates can be handled (i.e. can be read and verified) by current digital certificate management software such as OpenSSL. Also, we have relied on OpenSSL implementation for different cryptographic primitives. For implementing biotokens and ABCS subsystems, we chose to use the Biotope® as the underlying key-binding biometric template protection scheme. The Biotope® library implements a fingerprint version of the Bipartite Biotoken [14].

Our implementation of BKI supports both user and application interfaces. The user interface is designed as Command Line Interface (CLI). It allows end users and CAs to initiate commands for different BKI operations. The CLI is just a basic wrapper using the Application Programming Interface (API) which allows other software to use the BKI data types and perform different BKI operations. The source code for the BKI will be made open source, although it depends on non-open source libraries.

3 Trusted Biometric Web Identities (Trusted-BWI)

In this section, we introduce our proposed secure biometric web services: Trusted-BWI. Trusted-BWI is security and privacy-enhanced biometric web services that are designed to protect the privacy of users by protecting their biometric data. Trusted-BWI does not use raw or invertible representation of biometric data (i.e. images or invertible biometric templates). Instead, Trusted-BWI relies on BKI and its biotoken or ABCS subsystem for exchanging and storing biometric data. Using biometric certificates also enhances the trust level of remote biometric services (i.e. biometric enrollment). Also, using BKI's biometric certificates allows Trusted-BWI to support secure biometric sensors that perform cryptographically secured on-chip matching and do not disclose any biometric data. Figure 1 illustrates an overview of Trusted-BWI web services.

Trusted-BWI defines secure biometric enrollment and verification services. The enrollment service leverages BKI's biometric certificates in order to enhance its level of trust. Also, the enrollment service can be performed with or without authenticating the user. On the other hand, the verification service supports three different secure biometric verification protocols. The following sections describe the design of Trusted-BWI's enrollment and verification services.

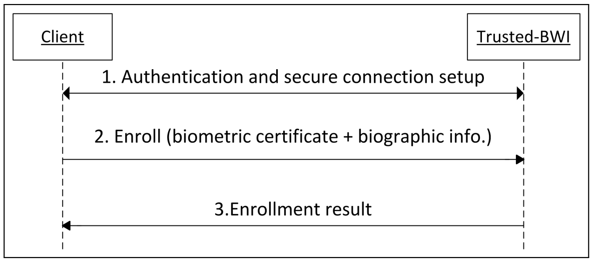
Client
Trusted-BWI
1. Authentication and secure connection setup
2. Enroll (biometric certificate + biographic info.)
3.Enrollment result

Figure 6. Sequence diagram of Trusted-BWI enrollment service.

3.1 Enrollment Service

Trusted-BWI provides a privacy and trust enhanced biometric enrollment service. The biometric enrollment service requires the client to have a biometric certificate with at least one biometric extension that contains either a biotoken or biometric public key. In addition to protecting biometric data, using biometric certificates has two additional advantages. Firstly, requiring a biometric certificate with a high level of CA identity proofing enhances the trust of remote biometric enrollment. This prevents users from spoofing other people biometrics. Secondly, biometric certificates, with their ABCS subsystem, support users of secure biometric sensors with cryptographically secured on-chip matching. This allows users to use the biometric enrollment service without risking their biometric data or lowering the level of security of the biometric enrollment services.

If the user does not have a biometric certificate, the Trusted-BWI service provider can act as a CA and issue biometric certificates for its users. As previously described in section 2.1, a service provider, if decided to act as a CA, can define its policy regarding the identity proofing level required to certify users. For example, a service provider can accept remote user certification with or without authenticating user's biometric or documents.

Figure 6 illustrates the synchronous enrollment service. The client requests the enrollment service passing the user's biometric certificate along with any biographic data required for enrollment (i.e., name, gender, and date of birth). The biometric certificate can be sent without protection, whereas the biographic data needs to be protected. A secure transport protocol (i.e., SSL) should be used for this purpose. The enrollment service enrolls the user (i.e., by adding the user's biometric certificate to a database) and responds to the client with the result of the enrollment process. Optionally, the enrollment service can biometrically authenticate the user. The biometric authentication can be performed remotely by sending a cryptographic

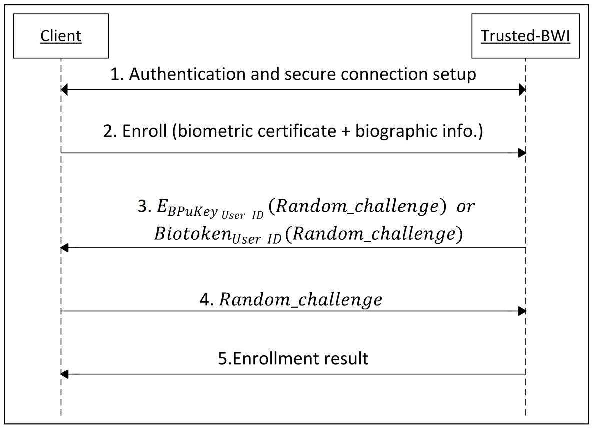
Client
Trusted-BWI
1. Authentication and secure connection setup
2. Enroll (biometric certificate + biographic info.)
3. $E_{BPuKey_{User\ ID}}(Random\_challenge)$ or
$Biotoken_{User\ ID}(Random\_challenge)$
4. $Random\_challenge$
5.Enrollment result

Figure 7. Sequence diagram of Trusted-BWI enrollment service with user authentication.

challenge to the user. The challenge is embedded into the user biotoken $Biotoken_{UserID}(Random\_challenge)$ or encrypted using the biometric public key$E_{BPuKey_{UserID}}(Random_challenge)$. The user can extract the challenge by applying his/her biometric to the biotoken that embeds the challenge or decrypting the challenge using the biometric private key. This allows the enrollment service to verify the biometric extension attached to the user's biometric certificate. Figure 7 shows the sequence diagram of the enrollment service with user authentication.

3.2 Verification Service

Trusted-BWI defines a secure biometric verification service that respects the privacy of biometric data. Instead of sending raw or invertible representations of users' biometrics for verification, Trusted-BWI uses biotokens or a remote biometric authentication protocol such as the authentication protocol introduced in section 2.3. The following subsections introduce three variations of the Trusted-BWI verification service.

3.2.1 Verification Service Using Biotokens

In this verification service, the user passes the subject ID along with a newly generated biotoken to the verification service. The received newly generated biotoken is matched against the user's stored biotoken. Then the user is notified about the verification result. Figure 8 illustrates the sequence diagram of this verification service. This verification service enhances the privacy by not sending raw or invertible representations of users' biometric data.

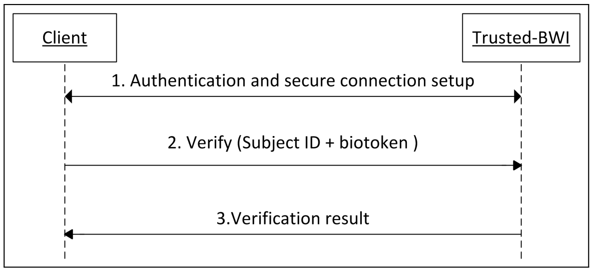
Client
Trusted-BWI
1. Authentication and secure connection setup
2. Verify (Subject ID + biotoken)
3.Verification result

Figure 8. Sequence diagram of Trusted-BWI verification service using biotokens.

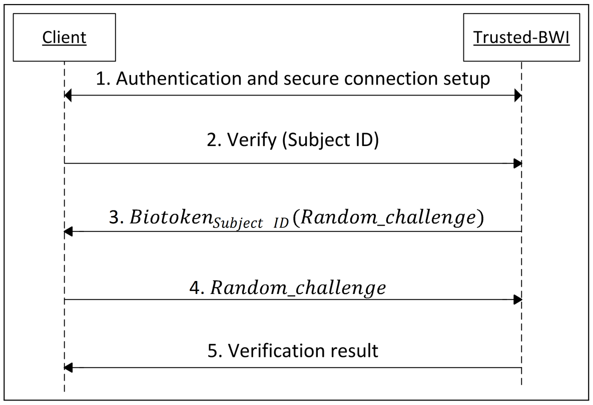
Client
Trusted-BWI
1. Authentication and secure connection setup
2. Verify (Subject ID)
3. $Biotoken_{Subject\ ID}(Random\_challenge)$
4. $Random\_challenge$
5. Verification result

Figure 9. Sequence diagram of Trusted-BWI verification service relying on challenge and response authentication protocol using biotokens.

3.2.2 Verification Service Relying on Authentication Protocol Using Biotokens

In this verification service, no biometric data is sent for verification. Instead, a remote biometric authentication protocol is used for verification. The user starts by sending the subject ID to the verification service. The verification service responds with a cryptographic challenge embedded into the user's biotoken$Biotoken_{SubjectID}(Random_challenge)$. The user can only obtain the challenge by applying his/her biometric in order to release the challenge from the biotoken. If the user is able to recover the challenge successfully, the user sends back the recovered challenge to the verification service. The verification service, in turn, verifies the returned challenge and notifies the user about the verification result. Figure 9 illustrates the sequence diagram of this verification service.

3.2.3 Verification Service Relying on Authentication Protocol Using BKI's ABCS

In this verification service, a remote biometric authentication protocol using BKI's ABCS (i.e., biometric public and private key) is used. The user starts with sending the subject ID to the verification service. The verification service responds with a cryptographic challenge encrypted using the user biometric public key $E_{BPuKey_{SubjectID}}(Random\_challenge)$. The user can only obtain the challenge by using his/her biometric private key. The user needs to authenticate, biometrically, to ABCS in order to use the biometric private key for encryption or decryption (i.e., to a secure biometric sensor with hardware trusted module). If the user is able to decrypt and obtain the challenge, the user sends back the recovered challenge to the verification service. The verification service, in turn, verifies the returned challenge and notifies the user about

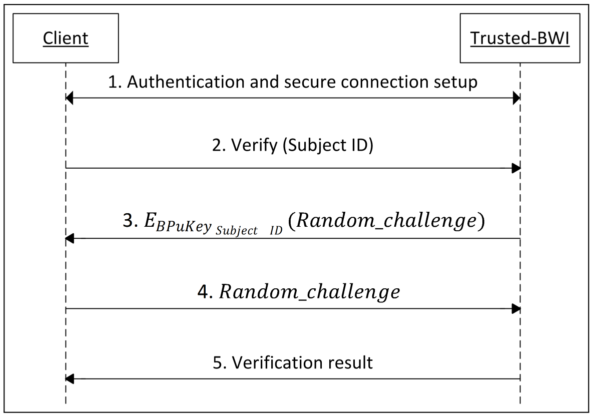
Client
Trusted-BWI
1. Authentication and secure connection setup
2. Verify (Subject ID)
3. $E_{BPuKey_{Subject\ \ ID}}(Random\_challenge)$
4. $Random\_challenge$
5. Verification result

Figure 10. Sequence diagram of Trusted-BWI verification service relying on challenge-and-response authentication protocol using BKI's ABCS.

the verification result. Figure 10 illustrates the sequence diagram of this verification service.

4 Discussion and Conclusion

Strong web identities, biometric web services, and remote biometric transactions in general, face many challenges in terms of privacy, trust, and compatibility with biometric sensors. In this paper, we focused on addressing these challenges, and many other problems, that slow the adoption of biometric web services and biometrics technology in general. In order to achieve our objectives, we introduced two main contributions.

Firstly, we proposed an enhanced design of the BKI framework. Our design of a BKI framework aims to address the privacy, trust, and compatibility problems of remote biometric transactions. The new BKI takes into account critical aspects of enrollment while still protecting the privacy aspect of the biometric data. The biometric certificate, as the core element of BKI, does not include any representation from which one effectively extracts biometric data. Moreover, the new enhanced BKI addresses the trust problem of remote biometric enrollment by introducing the CA identity proofing extension to the biometric certificate. The CA identity proofing extension defines how the CA has performed the identity proofing for the certified user. This extension can help any third party to determine the trustworthiness associated with a biometric certificate. In addition to enhancing the privacy and trust, the new enhanced BKI introduces ABCS, enhancing the level of compatibility with biometric sensors by supporting the new generation of the secure biometric sensors with cryptographically secured on-chip matching.

Leveraging our new enhanced BKI, we proposed the Trusted-BWI as biometric web services with a high level of security, privacy, and trust. Trusted-BWI leverages BKI's biometric certificates and their attached biotokens or ABCS subsystems instead of using raw or invertible representations of biometric data. Thus, Trusted-BWI provides high security and privacy with respect to the sensitive nature of users' biometrics data. Trusted-BWI defines a secure and trusted biometric enrollment and verification services. As a result of leveraging BKI, these secure biometric services support users of secure biometric sensors with cryptographically secured on-chip matching.

References

[1] American National Standard for Information Technology - Biometric Identity Assurance Services (BIAS). (INCITS 442-2010), 2010.

[2] Information Technology - Security Techniques - Biometric Information Protection Standard. (ISO/IEC 24745), 2011.

[3] Personal Identity Verification (PIV) of Federal Employees and Contractors. (FIPS PUB 201-1), 2011.

[4] OASIS Standard for Biometric Identity Assurance Services (BIAS) SOAP Profile Version 1 . 0. 2012.

[5] Biometric Identity Assurance Services (BIAS) Reference Implementation, 2013.

[6] M. Boshra, R. S. Brandt, J. C. Lee, G. T. Minteer, G. S. Porter, A. J. Vandamia, and J. R. Waldron. Finger Sensing Apparatus using Encrypted user Template and Associated Methods. (US 8,145,916), 03 2012.

[7] E. Dawson, J. Lopez, J. A. Montenegro, and E. Okamoto. BAAI: Biometric Authentication and Authorization Infrastructure. In *Information Technology: Research and Education, 2003. Proceedings. ITRE2003. International Conference on*, pages 274–278. IEEE, 2003.

[8] A. K. Jain, K. Nandakumar, and A. Nagar. Biometric Template Security. *EURASIP Journal on Advances in Signal Processing*, 2008(1):579416, 2008.

[9] G. Martinez-Silva, F. Rodriguez-Henriquez, N. Cruz-Cortes, and L. Ertaul. On the Generation of X.509v3 Certificates with Biometric Information. Technical report, Citeseer.

[10] R. Perez, R. Sailer, and L. van Doorn. vtpm: virtualizing the trusted platform module. In *Proc. 15th Conf. on USENIX Security Symposium*, pages 305–320, 2006.

[11] L. A. Reinert and S. C. Luther. User Authentication Techniques Using Public Key Certificates. Technical report, National Security Agency - Centeral Security Service, 1997.

[12] T. E. I. ROWLEY. High Security Biometric Authentication using a Public Key/Private Key Encryption Pairs. (WO 2000/065770), 11 2000.

[13] W. Scheirer, B. Bishop, and T. Boult. Beyond PKI: The Biocryptographic Key Infrastructure. In *Proceedings of the IEEE International Workshop on Information Forensics and Security (WIFS)*, pages 1–6, 2010.

[14] W. Scheirer and T. Boult. Bipartite biotokens: Definition, Implementation, and Analysis. *Advances in Biometrics*, pages 775–785, 2009.

[15] S. Thom, J. Cox, D. Linsley, M. Nystrom, H. Raj, D. Robinson, S. Saroiu, R. Spiger, and A. Wolman. Firmware-based trusted platform module for arm processor architectures and trustzone security extensions. (20130031374), January 2013.