Biometric Electronic Signature Security[1]

Phillip H. Griffin

Griffin Information Security, 1625 Glenwood Avenue, Raleigh, NC 27608, USA
phil@phillipgriffin.com

Abstract. This paper describes the application of biometric-based cryptographic techniques to create secure electronic signatures on contract agreements of any kind or format. The described techniques couple password and biometric authentication factors to form a Biometric Authenticated Key Exchange (BAKE) protocol. The protocol provides mutual authentication and multi-factor user authentication, and defeats phishing and man-in-the-middle attacks. The operation of BAKE establishes a secure channel of communications between two parties. This channel provides confidentiality for the users authentication credentials and the contract agreement the user intends to sign. By including an indication of the users intention to conduct an electronic transaction and the users acceptance of the terms of the included contract agreement, the described application complies with the Uniform Electronic Transaction Act (UETA) and Electronic Signatures in Global and National Commerce (ESIGN) Act requirements. The biometric electronic signature described in this paper is suitable for use in Cloud environments and in blockchain and Distributed Ledger Technology smart contract applications.

Keywords: authentication · biometrics · cryptography · e-signature · security

1 Introduction

User authentication data collected by biometric sensors can be rich in information content. Biometric sensor data can contain a biometric sample of an individual. This sample can be presented by a user to an access control system as a "something-you-are" identity authentication factor. Biometric matching techniques can make use of the provided sample to authenticate the identity of the user against a previously enrolled biometric reference. The same biometric sensor data can contain additional identity authentication information, such as user knowledge in the form of a weak secret shared by the user and an authentication system.

User knowledge, such as passwords, "passphrases and Personal Identification Numbers (PIN) are examples of weak secrets" [1]. Weak secrets are commonly used as authenticators for access control since they are convenient for people to use. These secrets are considered 'weak' because they "can be easily memorized" and recalled by users, and because they are often selected from "a relatively small set of possibili-

[1] *Submitted to 9th International Conference on Applied Human Factors and Ergonomics (AHFE 2018) - Human Factors in Cybersecurity Conference - Personal Copy*

ties" [2] that can make them easily guessed. A weak secret can serve as a "something-you-know" authentication factor that can be collected directly from a user input device, or extracted from biometric sensor data [3].

When weak secrets are extracted from biometric sensor data they can be coupled with biometric matching to provide two authentication factors, "something-you-know" and "something-you-are". Extraction of this user knowledge from biometric sensor data allows two factors to be derived from a single user interaction with a data collection device. This technique can be incorporated into the design of an access control system to provide strong, two-factor authentication that does not diminish the user experience of a single factor authentication system. Extracted user knowledge can also serve as the shared secret needed to operate an Authenticated Key Exchange (AKE) protocol, such as the Biometric AKE (BAKE) protocol [3] and to establish the secure channel between two communicating parties needed to perform an electronic signature transaction.

Protocols. The Password AKE (PAKE) protocol has been defined internationally in both the ISO/IEC 11770-4 [2] standard and the ITU-T X.1035 [4] recommendation. PAKE can be operated using a weak secret provided directly from biometric sensor data by extraction (i.e., using BAKE), or operated with user knowledge entered from a keyboard or touch screen device that is separate from a biometric sensor. PAKE and BAKE can be used to establish "a symmetric cryptographic key via Diffie-Hellman exchange" [4].

The BAKE protocol depends on PAKE for its key exchange mechanism. PAKE relies on a weak secret input to a Diffie-Hellman key exchange protocol for cryptographic key establishment. These AKE protocols allow remote communicating parties to "establish a secure communication channel" without the need to rely "on any external trusted parties" [5]. Diffie-Hellman key exchange is at the heart of both BAKE and PAKE, as illustrated in Fig. 1.

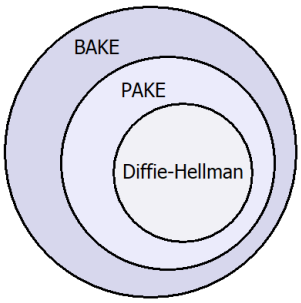

Fig. 1. Relationship of the Biometric Authenticated Key Exchange (BAKE) and Password Authenticated Key Exchange (PAKE) protocols to the Diffie-Hellman protocol.

In resource constrained environments, such as high-volume transaction systems, smart cards, or Internet of Things (IoT) environments, this attribute can provide a significant benefit [6]. PAKE does not require the cost of digital certificates for entity authentication, or on the ability of entities to access an always available Public Key Infrastructure (PKI) for certification path validation, or on the assumption that the

user has access to a reliable and fully functional PKI. The use of PKI-based methods can " require too many computation, memory size, and bandwidth resources" for use in IoT environments [7].

Diffie-Hellman is a key establishment technique that "provides forward secrecy, prevents user credentials from being exposed during identity authentication attempts, and thwarts man-in-the-middle and phishing attacks" [1]. By using Diffie-Hellman for key establishment, a secure channel can be established between two parties for subsequent communications. Key establishment is then based “on a shared low-entropy password”, a weak secret known to both parties [5]. This shared secret input to the Diffie-Hellman protocol through BAKE, then PAKE allows these protocols to provide implicit identity authentication [5].

The BAKE protocol extends the single factor PAKE protocol to provide strong, two-factor authentication. Both BAKE and PAKE provide mutual authentication through challenge-response messages exchanged securely between the parties. The confidentiality of the challenge-response, the user credentials, and any included content are protected from attack by encryption during transfer. A high level description of the BAKE protocol processing steps is provided in Fig. 2.

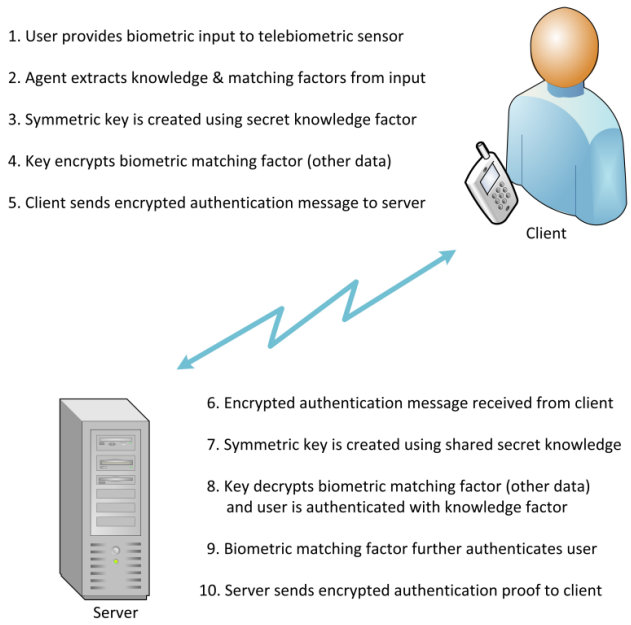

Fig. 2. Biometric Authenticated Key Exchange (BAKE) authentication processing.

One example of BAKE authentication processing uses "speech recognition along with speaker recognition biometrics to provide two-factor authentication" [8]. The two-factor authentication input by the user to this process can rely on data extracted "from a single biometric sensor" [8]. The *something-you-know* authenticator comes from "the words spoken by a user, which form the knowledge string" used in BAKE

"to create a symmetric encryption key" [8]. The *something-you-are* authenticator "contains biometric matching data" [8].

When the included data in step 4 of Fig. 2 is a user agreement or contract, the BAKE and PAKE authentication protocols become a secure foundation for the implementation of electronic signatures. Identity authentication of contract signatories is a traditional requirement of contract law worldwide, and for electronic signatures care must be taken to insure that "the method used to identify the signer is reliable" [9]. Additional assurance against subsequent attempts to repudiate an e-signed agreement can be gained by the inclusion of additional content in the encrypted BAKE message.

2 Biometric Electronic Signatures

The meaning of the term electronic signature (e-signature) varies by legal jurisdiction. In the United States, two acts specify the term, the Electronic Signatures in Global and National Commerce Act (E-Sign) and the Uniform Electronic Transaction Act (UETA). These acts describe an e-signature as "any process, symbol or electronic sound performed by an individual and associated with information that the individual agrees to accept and sign, and an indication of intention to conduct an electronic transaction" [10].

A valid e-signature can be implemented to authenticate the identity of the signer using a number of different techniques. These techniques include "a digital signature, a digitized fingerprint, a retinal scan, a pin number", or "a digitized image of a handwritten signature that is attached to an electronic message" [9]. A "common method of creating a valid signature is the 'shared secrets' method", which both authenticates the signer and uses "passwords or credit card numbers to establish the necessary intent to conclude a transaction" [11]. These characteristics make BAKE and its embedded PAKE protocol a suitable mechanism for the implementation of e-signatures.

There are no e-signature security requirements for protecting the signers "private identifying information such as private keys and passwords" [11]. There are no requirements for safeguarding the user against phishing or man-in-the-middle attacks, the use of strong, multi-factor authentication, forward secrecy of cryptographic keys, or the provision of user assurance through mutual authentication. Ideally, an optimal e-signature solutions would meet all of these security requirements as well as the e-signature requirements specified in E-Sign and UETA.

The BAKE protocol can meet all of these requirements and address the security risks associated with e-signatures. These risks include the risk of repudiation of a signed contract and the failure to properly authenticate the e-signer. Since BAKE provides mutual authentication, e-signers can "identify themselves to a server and gain assurance that the server they are trying to connect to is not an imposter" [12]. BAKE provides the relying party of a contract with strong multi-factor authentication of the e-signer, but "does not require changes in user behavior or to the user authentication experience" [12].

Proof that a "person approved a particular electronic document might be gathered in many different ways" [13]. To mitigate the risk of later repudiation, a relying party should also document the signers intention to conduct an electronic transaction and their acceptance of the terms and conditions of the e-signed agreement. Biometric

voice samples acquired from the e-signer can be used for this purpose if they are transferred and stored securely. A relying party can use this documentation to reduce the risk of repudiation, since the documentation may be replayed or used for biometric matching to demonstrate evidence of e-signer consent.

Standardization. The draft 2018 revision of the X9.84 Biometric Information Management and Security standard [14] specifies "three new biometric-based e-signature techniques" [10]. These techniques include two that are PKI-based, Biometric Electronic Signature Token (BEST) and Signcrypted BEST (SBEST). The standard also specifies the "biometric electronic-signature authenticated-key exchange (BESAKE)" protocol [10] described in this paper. A high level description of the processing steps of the BESAKE protocol is provided in Fig. 3.

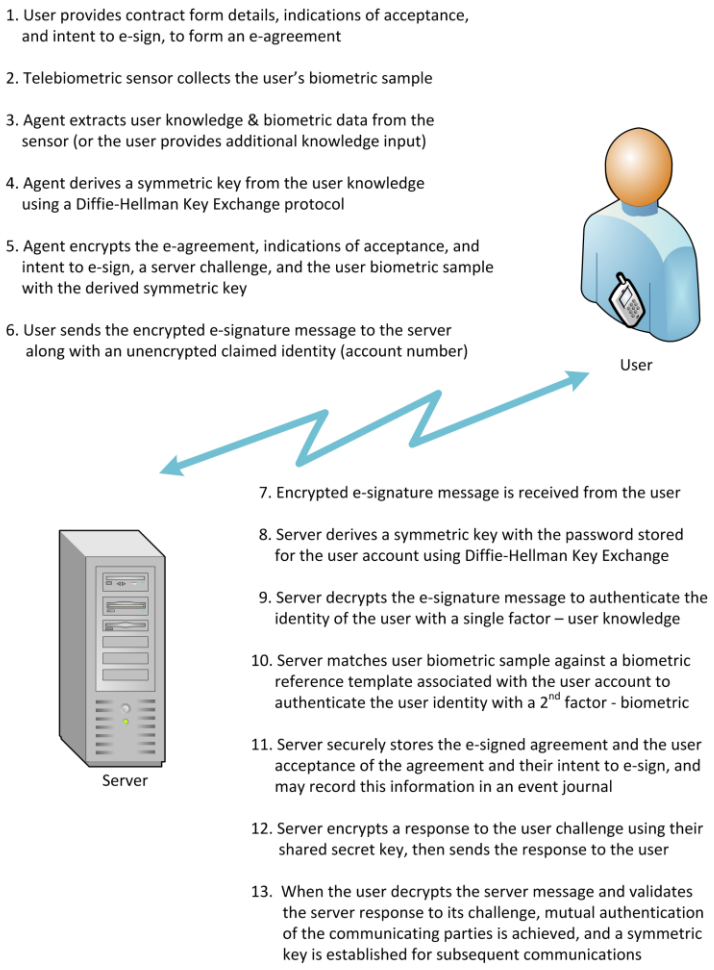

Fig. 3. Biometric Electronic Signature Authenticated Key Exchange (BESAKE) protocol.

The BESAKE protocol builds upon BAKE authentication to form an electronic signature protocol. The key differences in these protocols are captured in steps 1, 5, and 11 in Fig. 3. To meet the requirements of the E-Sign and UETA acts, the intention of the signatory to perform an electronic transaction and their acceptance of the terms of the agreement being signed have been captured along with the agreement. The confidentiality of these values are protected by encryption during transfer from the signer to the relying party or server.

To mitigate the risk of subsequent repudiation of the agreement, the relying party can store and log the details of the e-signing event. Date and time, location, and other information may be included in the log, and coupled with the agreement. Digital signatures and encryption may be used to protect the authenticity, data integrity and confidentiality of this information, so that it can be relied on by a third party. Other security controls may also be employed as appropriate to manage security risk.

3 Biometric Intention and Acceptance

A commonly used method for capturing the intention of a user to conduct an electronic transaction and their acceptance of the terms of an agreement is to present the user with text associated with check boxes. To complete a contract a user may be required to check the boxes before completing the transaction to indicate intent to sign and acceptance of an offer.

Biometrics can be used to provide stronger evidence of the user intent to e-sign and accept an agreement. The use of biometrics can enhance the e-signature experience.

Abstract Schema. Different types of exchanges used to document a users acceptance of terms and their intention to sign electronically can be collected by a user agent on the client device. These exchange types include biometric and traditional exchanges, such as text entries, check boxes and button selections made by the user in response to presented information in a screen format. The following ASN.1 [15] `Exchanges` Information Object Set defines an extensible set of exchange objects. This set is used to constrain the valid components of type `Exchange` based on the ASN.1 Information Object Class `&Type` and `&id` fields.

Example of an abstract schema [15] for unambiguous transfer of a biometric user agreement to terms and intention to electronically sign a contract based on the Abstract Schema Notation One (ASN.1) standard.

```
AgreeAndIntendToESIGN ::= SEQUENCE {
   agreeToTerms  Exchange,
   intendToSign  Exchange
}

Exchange ::= SEQUENCE {
   responseID    EXCHANGE.&id({Exchanges}),
```

```
   userResponse  EXCHANGE.&Type({Exchanges}{@responseID})
}


Exchanges EXCHANGE ::= {
   { BinaryData  IDENTIFIED BY id-Voice }        |
   { BinaryData  IDENTIFIED BY id-FaceAndVoice } |
   { UTF8String  IDENTIFIED BY id-TextEntry }    ,

   ...  -- Expect additional exchange objects --
}

BinaryData ::= OCTET STRING (SIZE(1..MAX))

EXCHANGE ::= TYPE-IDENTIFIER  -- ISO/IEC 8824-2, Annex A
```

In this schema, text exchanges are collected as character strings that can represent characters from any national language. The information object identifier `id-Voice` indicates the voice of the e-signer is used to document the exchange. Multi-modal biometric exchanges are also supported by the schema. Face and voice biometrics exchanges can be captured using the `id-FaceAndVoice` identifier. The extension marker, `"..."` instructs messaging tools to expect additional `Exchanges` information objects, allowing support for additional mechanism to be added by an implementer as needed.

4 Conclusion

Cryptographic and biometric identity authentication techniques commonly used for access control can be extended to implement secure, e-signature protocols. These protocols can be inexpensive to implement and convenient for e-signers to use. Since the confidentiality of user credentials, personally identifiable information, and the terms of agreement are protected using encryption, biometric e-signatures are suitable for use in smart contract, distributed ledger, and cloud environments. Both PAKE and BAKE authenticated key exchange protocols authenticate the identity of electronic signers, and both provide the e-signer with the assurance of mutual authentication.

Electronic signature techniques based on PAKE and BAKE can defeat phishing and man-in-the-middle attacks. With PAKE and BAKE, user password and biometric credentials are never revealed to an attacker during an authentication attempt. With both protocols, the confidentiality of an agreement is ensured by strong cryptography and forward secrecy when fresh values are used.

The intention of a user to electronically sign, and their agreement to the terms and conditions of a contract can be documented using biometric technology and protected from loss of confidentiality by the BAKE protocol. This use of biometrics can provide greater protection of a relying party against future attempts by the signer to repudiate the terms of an agreement or their intention to sign than check boxes and similar indications.

References

1. Griffin, P.H.: Adaptive weak secrets for authenticated key exchange. In: *Advances in Human Factors in Cybersecurity*, pp. 16-25. Springer Switzerland (2017)
2. International Organization for Standardization/ International Electrotechnical Commission: ISO/IEC 11770-4 Information technology – Security techniques – Key Management – Part 4: Mechanism based on weak secrets (2017)
3. Griffin, P.H.: Biometric knowledge extraction for multi-factor authentication and key exchange. Procedia Comput. Sci. 61, 66–71 (2015). Complex Adaptive Systems Proceedings, Elsevier B.V.
4. International Telecommunications Union - Telecommunications Standardization Sector (ITU-T): ITU-T Recommendation X.1035: Password-authenticated key exchange (PAK) protocol (2007)
5. Hao, F., Shahandashti, S.F.: The SPEKE protocol revisited. In: Chen, L., Mitchell, C. (eds.) Security Standardisation Research: First International Conference, SSR 2014, pp. 26–38, London, UK, 16–17 December 2014. https://eprint.iacr.org/2014/585.pdf. Accessed 24 Dec 2017
6. Griffin, P.H.: Biometric-based cybersecurity techniques. In: *Advances in Human Factors in Cybersecurity*, pp. 43-53. Springer Switzerland (2016)
7. Griffin, P.H.: Secure authentication on the internet of things. In: IEEE SoutheastCon, April,2017
8. Griffin, P.H.: Security for ambient assisted living: Multi-factor authentication in the internet of things. In: IEEE Globecom, December, 2015
9. Blythe, S. E.: Digital signature law of the United Nations, European Union, United Kingdom and United States: Promotion of growth in E-commerce with enhanced security. In: Richmond Journal of Law & Technology, 11(2), 6 (2005). https://scholarship.richmond.edu/cgi/viewcontent.cgi?referer=https://scholar.google.com/&httpsredir=1&article=1238&context=jolt. Accessed 12 Feb 2018
10. Griffin, P.H.: Biometric electronic signatures. Inf. Syst. Secur. Assoc. (ISSA) J. 15(11) (2017)
11. Stern, J. E.: The Electronic Signatures in Global and National Commerce Act. In: Berkley Technology Law Journal. 391-414 (2001).
12. Griffin, P.H.: Transport layer secured password-authenticated key exchange. Inf. Syst. Secur. Assoc. (ISSA) J. 13(6) (2015)
13. Wright, B.: Eggs in Baskets: Distributing Risks of Electronic Signatures. In: John Marshall Journal of Computer and Information Law. 15(189), (1996).
14. Accredited Standards Committee (ASC) X9 Financial Services: X9.84 Biometric Information Management and Security.
15. Larmouth, J.L.: ASN.1 Complete. Morgan Kaufmann, London (2000)