Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 00 (2014) 000–000

Procedia Computer Science

www.elsevier.com/locate/procedia

Complex Adaptive Systems, Publication 4
Cihan H. Dagli, Editor in Chief
Conference Organized by Missouri University of Science and Technology
2014-Philadelphia, PA

Telebiometric authentication objects*

Phillip H. Griffin†

Griffin Information Security Consulting, 1625 Glenwood Avenue, Raleigh, NC 27608 USA

Abstract

This paper describes a method for achieving strong, low cost multi-factor authentication on the Internet of Things that is convenient for people to use. Authentication relies on tagged objects functioning with biometric sensors connected to a telecommunications network. Access control systems based on these telebiometric authentication objects do not require users to carry individually assigned security tokens, remember complex passwords, or possess and manage cryptographic keys and public key certificates. Authentication decisions are based on previously registered person-object associations created using cryptographic techniques that bind the biometric reference template of an individual to one or more tagged objects. Trusted person-object bindings are formed using digital signature or signcryption techniques based on certificates in a public key infrastructure. Cryptographic message syntax is defined that can be used to provide data integrity and origin authenticity services for telebiometric authentication objects and messages, and to protect the confidentiality of personally identifiable and other sensitive information.

Selection and peer-review under responsibility of scientific committee of Missouri University of Science and Technology.

Keywords: authentication; RFID; signcryption; telebiometrics

* Paper accepted for presentation at the "Conquering Complexity: Challenges and Opportunities" Missouri University of Science and Technology Complex Adaptive Systems Conference, Philadelphia, Pennsylvania, USA, November 3-5, 2014

† Corresponding author. Tel.: +1-919-291-0019.
E-mail address: phil@phillipgriffin.com

Selection and peer-review under responsibility of scientific committee of Missouri University of Science and Technology.

1. Identification

Individuals can be uniquely identified by their distinctive biometric traits. A biometric is a "measurable biological or behavioral characteristic, which reliably distinguishes one person from another"[1]. Biometric characteristics are used to identify an individual or to verify their claimed identity by matching a biometric sample against previously stored biometric reference information. Biometric matching can be performed using technologies such as fingerprints, speaker recognition, iris scans, and facial recognition. In an access control system, a biometric sample can serve as a *something-you-are* authentication factor.

A biometric reference template is created when an individual enrolls in a biometric system. Reference templates can be stored in a database to support subsequent biometric matching. Each template contains biometric data created with information extracted from biometric samples provided by an individual during enrollment.

When a biometric reference template is created, it is assigned a unique identifier and may be populated with other information that further identifies an enrollee. The ISO/IEC 19785 biometric information exchange standard defines a common reference template format. This standard template format contains an index field whose value uniquely identifies a specific instance of enrollment data for an individual[2]. The value of an index field indirectly identifies the person whose biometric sample matches the enrollment data in a given biometric reference template.

A value of the template index field can serve as a template database key in a biometric system. This key can be used to speed up the verification process when an individual asserts an identity claim, such as a claim on an account name or number. Any unique identifier can be used as the reference template index or database search key, including a fixed length cryptographic hash of a template, a Uniform Resource Locator (URL), or an information object identifier defined using Abstract Syntax Notation One (ASN.1). The value of a template index field is a constant that could be used to track or monitor an individual over time, and access to the value should be restricted and its confidentiality protected[1].

Physical objects in the Internet of Things (IoT) can be uniquely identified using Radio Frequency Identification (RFID) tags. Each RFID tag "transmits a unique serial number via radio waves to an interrogator, or reader"[3]. The tag allows identification of an object to which the RFID is attached or embedded. RFID tags are wireless computing devices "based on a microprocessor containing a data memory space"[3], making them suitable for use in a wide range of applications. A physical object in the IoT that is registered to an individual can "serve as a possession factor"[4] and can be used in an access control system as a low cost *something-you-have* authentication factor that eliminates the need for expensive individual tokens.

When an individual is enrolled in a biometric system, they can be associated with a set of physical objects using their unique biometric reference template identifier and one or more unique RFID serial numbers. These registered person-object associations can be used by that individual for multi-factor authentication. The list of registered physical objects associated with an individual can be modified over time to adapt to changing user access permissions. Modifications to the list of objects do not require that the individual reenroll in the biometric system.

2. Attributes

People have relationships with physical objects. They may own, lease, or rent objects, such as houses, automobiles, or hotel rooms. They may interact with objects around them based on their role, such as the role of a vehicle driver or passenger.

Groups of individuals may share relationships with the same object in the IoT. Some objects may be associated with a small finite list of people, such as the family members of a household who are allowed entry into a vehicle or home. A larger list of people might include those who share the role of employee, and who are authorized to enter a factory or office building. Some objects may be associated with a public role and shared more generally, perhaps by everyone who enters an airport or shopping center.

Roles can be represented in an access control system as signed attributes that are bound to a person-object association under a digital signature. A role attribute value might confer specific rights or privileges of an individual with respect to access to an object and its use (e.g., as object owner, lessor, lessee, guest, etc.).

Data privacy and information security management attributes may also be bound to a person-object association. Such attributes could include a privacy policy, "the number of authentication factors required for access, the number

of biometric match attempts allowed, or time of day usage restrictions"[5]. Other attributes might include the expected geographic location of an object or its security and safety configuration settings[6].

3. Association

A biometric reference template identifier and an RFID tag can be used to associate a particular person with a physical object[6], as shown in Fig. 1.

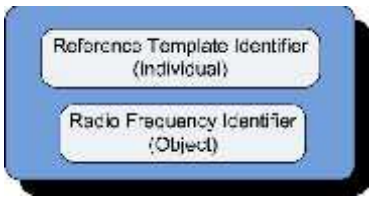

Fig. 1. Person-object association.

Person-object associations can be specified using a schema definition language such as Abstract Syntax Notation One (ASN.1)[7]. Formal schema definitions support automated processing by syntax checking and programming language code generation tools. Standardized schema definitions for information exchange can improve the likelihood of standards adopters creating solutions that interoperate.

Values based on ASN.1 schema types can be represented both in a compact binary format and in a verbose, human-readable Extensible Markup Language (XML) format. ASN.1 values can be readily converted between these formats. This feature allows information exchange applications to enjoy efficient binary transfer and compact storage of information without sacrificing the benefits of XML when needed.

A simple person-object association information object can be defined as an ASN.1 schema[5] as shown in Fig. 2.

```
SimpleAssociation ::= SEQUENCE {
   individual       BiometricTemplateID,
   physicalObjects  RFIDs
}

BiometricTemplateID ::= OCTET STRING

RFIDs ::= SEQUENCE (1..MAX) OF RFID

RFID ::= OCTET STRING
```

Fig. 2. Person-object association schema.

A value of ASN.1 type `SimpleAssociation` is defined as a pair of components, an `individual` associated with a series of one or more `physicalObjects`. Each physical object is identified as a value of type `RFID`. A biometric reference template of an individual is identified as a value of type `BiometricTemplateID`.

Applications can be expected to use person-object association objects in different ways. The association may be stored in the memory of an RFID tag or within a biometric reference template. Person-object associations may be stored in a database that is separate from the reference templates in the matching system of a biometric service provider[6].

A digital signature can cryptographically bind the identifier value of an RFID tag to a biometric reference template identifier[6]. Attributes of any kind or format needed by an application can be protected under this signature and bound to a person-object association. Verification of the binding can provide assurance to a relying party of the integrity and authenticity of a person-object association and any signed attributes bound to the object.

Digital signatures tied to certificates in a public key infrastructure can offer both data integrity and origin authenticity, and may allow applications to provide non-repudiation and other information security services.

Biometric samples contain personally identifiable information whose confidentiality should be protected using security controls such as limited access and data encryption.

The ISO 19092 standard requires that the confidentiality of biometric information be protected. ISO 19092 recommends digitally signing biometric information to ensure its integrity and authenticity, and to allow accidental or intentional modifications to be detected. This suggests that a sign-then-encrypt scheme is required to provide end-to-end protection of biometric reference template information and person-object associations. As an alternative to this approach, the SigncryptedData cryptographic message described in this paper can provide efficient, field level data confidentiality, integrity, and authenticity[8].

4. Signcryption

Signcryption is a hybrid cryptographic technique that provides an efficient means for both signing and encrypting information in a single operation. This combination of a digital signature with encryption is similar to the authenticated encryption (AE) mechanisms widely used in network security protocols on the Internet today. The use of AE includes a variant of the “MAC-then-encrypt (MtE)” mechanism used in the Secure Sockets Layer (SSL) protocol, the “Encrypt-then-MAC (EtM)” mechanism used in the Encapsulating Security Payload (ESP) protocol of Internet Protocol Security (IPsec), and the “Encrypt-and-MAC (E&M)” mechanism used in the transport layer of the Secure Shell protocol (SSH) [9].

Application of a signcryption cryptographic safeguard can help to ensure the “availability, confidentiality, integrity, authentication, unforgeability and non-repudiation”[10] of information assets. Unlike security safeguards that "rely on symmetric keys, the reliance of signcryption on asymmetric cryptography makes non-repudiation possible"[11]. Security services that provide non-repudiation can give a relying party reasonable certainty of the integrity and origin of information.

Efficient signcryption schemes “fulfill both the functions of digital signature and public key encryption in a single step, and with a cost, both in terms of modular exponentiation and message overhead, significantly smaller than that required by” traditional sign-then-encrypt techniques[12]. These efficiencies make signcryption ideal for use in the IoT where environments may be constrained by bandwidth limitations (e.g., wireless and mobile devices), high volumes of transactions (e.g., systems with large numbers of devices or users), or size or cost of storage (e.g., small devices, smart cards, etc.).

Signcryption schemes “achieve confidentiality and authentication simultaneously by combining public-key encryption and digital signatures, offering better overall performance and security” with lower computational cost and a smaller resulting cipher text[13]. This technique can replace the use of digital signature combined with encryption schemes, to make cryptographic protection feasible in environments where the use of such protection may have been prohibitive in the past. When a signcryption scheme is used, “encryption and signature are performed in a single logical step in order to obtain confidentiality, integrity, authentication and non-repudiation more efficiently than the sign-then-encrypt approach” [14]. Signcryption can be used in the IoT as a safeguard to mitigate the risks of unauthorized access, loss of trust in data sources, and undetected modifications of stored associations and authentication data transferred across open networks.

The ISO/IEC 29150 Signcryption information security standard provides a schema for signcryption mechanisms and cryptographic algorithm identification. However, no schema is provided for using signcryption in the secure messages and protocols needed to protect authentication data and person-object associations. Recently, a secure message schema for supporting signcryption techniques was proposed for standardization by the International Telecommunications Union (ITU) [11]. Subsequently, a new work item to develop a Cryptographic Message Syntax (CMS) standard was approved and assigned to ITU-T Study Group 17. This new joint ITU-T recommendation and ISO/IEC 24824-4 standard will include a new CMS type to support signcrypted data.

There are a “wide variety of signcryption schemes” with different sets of security properties and “relative advantages and disadvantages” [15]. One important advantage is that many “signcryption schemes require only a single key pair for each user”, which lowers implementation cost, while traditional sign-then-encrypt schemes require two: "one for encrypting and one for signing” [15]. Using a signcryption approach can minimize the cryptographic key management requirements needed to provide strong data protection in resource constrained environments. Properties of signcryption schemes can be useful in protecting personally identifiable biometric information or the identifiers

of objects tied to permanent locations. Signcryption can minimize exposure of plaintext tagged identifiers to prevent data aggregation that might be used for the tracking of individuals.

5. Secure message schema

A message schema for the secure exchange of signcrypted data has been proposed for standardization[11]. The proposed schema is defined as ASN.1 type SigncryptedData. The schema definition is based on the familiar SignedData type used to protect biometric information in the ISO 19092 biometric information management and security standard and several other international biometric and information security standards.

A secure signcryption message can exchange information in both XML markup and in a compact binary format using a single schema defined as an abstract syntax. A proposed schema was first presented at the ID360 Global Forum on Identity conference[8] in Austin at the University of Texas in 2012. An improved version of that schema, shown in Fig. 3, was presented to ITU-T Study Group 17 in January 2014 for inclusion in their draft CMS standard.

```
SigncryptedData ::= SEQUENCE {
   version                 Version,
   digestAlgorithms        DigestAlgorithms,
   encapsulatedContentInfo EncapsulatedContentInfo,
   certificates            Certificates  OPTIONAL,
   crls                    CRLs  OPTIONAL,
   signcrypterInfos        SigncrypterInfos
}

SigncrypterInfos ::= SET OF SigncrypterInfo

SigncrypterInfo ::= SEQUENCE {
   version             Version,
   signcrypterIDs      SigncrypterIDs,
   digestAlgorithm     [0] DigestAlgorithm  OPTIONAL,
   signedAttributes    [1] SignedAttributes  OPTIONAL,
   signatureAlgorithm  SignatureAlgorithm,
   signature           Signature,
   unsignedAttributes  [2] UnsignedAttributes  OPTIONAL
}

SigncrypterIDs ::= SEQUENCE {
   sender     KeyPairIdentifier,
   recipient  KeyPairIdentifier
}

KeypairIdentifier ::= CHOICE {
   issuerAndSerialNumber  IssuerAndSerialNumber,
   subjectKeyIdentifier   [0] SubjectKeyIdentifier,
   certificateHash        [1] CertificateHash
}
```

Fig. 3. SigncryptedData schema.

A value of ASN.1 type `SigncryptedData` is defined as a sequence of components. These components include the `version` of the syntax, the `digestAlgorithms` used in cryptographic operations, an `encapContentInfo` field for signcrypted content, optional digital `certificates` and certificate revocation lists (`crls`), and a `signcrypterInfos` field. The `signcrypterInfos` field contains one value of type `SigncrypterInfo` for each of one or more information exchange participants.

Each value of type `SigncrypterInfos` identifies the public-private key pairs of the message sender and recipient in a value of type `SigncrypterIDs`. A message sender uses his or her own public and private keys along with the public key of the recipient to encrypt and sign plaintext content. The message recipient uses the public key of the sender with his or her own public and private keys to verify the signature and recover the encrypted plaintext.

Three modes of processing for a secure SigncryptedData type have been proposed that can be useful in a telebiometric authentication system: "*signcrypted-content*, *signcrypted-attributes*, and *signcrypted-components*"[16]. The *signcrypted-components* mode of SigncryptedData supports "signcryption of selected components of a biometric transaction or reference template"[16] and the field level signcryption of other types of information. Using the *signcrypted-components* mode, one or more components of an information object of any type or format are signcrypted, then "the resulting object is bound to one or more attributes under a digital signature"[16].

Attributes of any type or format can be bound to a person-object association using the SigncryptedData type. The X.509 attribute certificate standard defines an ASN.1 schema for roles. This schema has been widely adopted and is used to specify digital signature policies in the European Telecommunications Standards Institute (ETSI) Electronic Signatures and Infrastructures (ESI) standard. X.509 style roles can be bound to person-object associations as SigncryptedData attributes and used in role-based access control (RBAC), and in attribute-based access control (ABAC) systems, which “require no advanced knowledge of requestors” and allow an individual’s attributes to be “correlated from multiple sources” [17].

6. Implementation

Many access control architectures could make use of biometric associated objects. Though not a complete architecture, the access control system context diagram shown in Fig. 4 provides a black box view as an example of one possible approach. This view depicts at a high level the interactions between an access control system and its external components, and illustrates the control and information flows between the system and these components.

Fig. 4. Access control system context.

Four components interact within the access control system: Certificate Authority (CA), Biometric Service Provider (BSP), Person-object Associations, and Telebiometric Authentication Object System. The CA provides certificate management services and securely maintains the cryptographic keys needed to provide its services. The CA publishes revocation lists, and may provide certificate validation services.

The BSP maintains a database of biometric reference templates and performs biometric matching services by comparing biometric match data provided by a user during an authentication attempt. The BSP returns a Yes/No response to the access control system that indicates whether the biometric match was successful.

There is one person-object association record for each user enrolled in the biometric system. Each record contains a list of RFID-identified objects. This list is associated with the unique biometric reference template identifier of an enrollee in a reference template database. After a successful biometric authentication attempt has been indicated by the BSP, the association record for the matched user is located, then searched for the RFID tag values provided in an authentication request sent from a telebiometric authentication object system. A list of matching tags is returned to the access control system.

The telebiometric authentication object system collects biometric samples from a person using one or more biometric sensors. These samples and a list of the unique identifiers from one or more nearby tagged objects are used to create an authentication request message. Prior to sending the request message, the telebiometric authentication object system may mutually authenticate the recipient server using a protocol such as Transport Layer Security (TLS). The telebiometric authentication object system receives a response message containing the user authentication results. This message contains a list of zero or more tagged objects the user is permitted to access.

During enrollment in a biometric system, a user provides biometric samples to a BSP who creates a biometric reference template and stores the template securely for subsequent biometric matching. Reference templates should be signed and their personally identifiable information should be encrypted. Three modes of processing can be used with the SigncryptedData type. The *signcrypted-components* mode can be used to protect biometric reference templates and to ensure their "authenticity and integrity, as well as the confidentiality of their biometric data"[11].

Authentication request messages are sent from the telebiometric authentication object system to an access control service that manages the authentication process. The authentication process relies on a BSP for biometric matching and a person-object association registry for tagged object matching. This message can be defined using the ASN.1 schema in Fig. 5:

```
AuthenticationRequest ::= SEQUENCE {
  matchingMessages  Nonce,
  biometricSamples  BiometricSamples,
  associatedThings  RFIDs,
  somethingYouKnow  OCTET STRING  OPTIONAL,
  assertedIdentity  OCTET STRING  OPTIONAL
}

Nonce ::= OCTET STRING

BiometricSamples ::= SEQUENCE SIZE(1..MAX) OF BiometricObject

BiometricObject ::= SEQUENCE {
  biometricType  RELATIVE-OID,
  biometricData  OCTET STRING
}
```

Fig. 5. Authentication request schema.

Authentication requests contain personally identifiable and other sensitive information. The `matchingMessages` component contains control information to allow pairing of request response messages and to prevent message replay attacks. The `biometricSamples` and `associatedThings` components contain information that can identity a user and the physical objects they may intend to access. The confidentiality of these components should be protected. The `somethingYouKnow` component contains an optional value of type `OCTET STRING`. When present, this value contains a personal identification number (PIN), a password, or a passphrase. Component `assertedIdentity` contains an optional value of type `OCTET STRING`, which can contain an account name or other indication of a claimed identity.

Values of type `AuthenticationRequest` should be signed and encrypted to ensure their integrity, authenticity, and confidentiality. The *signcrypted-content* mode of SigncryptedData can be used to protect an authentication request message when there are no attributes that require protection. When protected attributes are required, the message sender can use the *signcrypted-attributes* mode.

An authentication response message can be defined using the following ASN.1 schema:

```
AuthenticationResponse ::= SEQUENCE {
   matchingMessages  Nonce,
   authorizedThings  RFIDs  OPTIONAL
}
```

Fig. 6. Authentication response schema.

The `matchingMessages` component is used to pair the response message to a specific authentication request. If present, the optional `authorizedThings` field contains a list of one or more RFID tag values that the user is authorized to access. There may be more or less objects in the list than sent in the authentication request to eliminate the need for subsequent requests.

Values of type `AuthenticationResponse` should be signed and encrypted to ensure their integrity, authenticity, and confidentiality. Either the *signcrypted-content* mode or the *signcrypted-attributes* mode of SigncryptedData can be used to protect an authentication response message.

6. Conclusion

A biometric sample matched to a biometric reference template is a *something-you-are* authentication factor that can uniquely identify an individual. An RFID tag can uniquely identify a physical object. Tagged objects registered to an individual can be used by that individual as a *something-you-have* authentication factor. When coupled with a *something-you-are* biometric sample and a *something-you-know* secret value, two and three factor authentication solutions are possible.

Tagged objects functioning with biometric sensors connected to a telecommunications network can be used to provide multi-factor access control systems in the Internet of Things. A tagged object can serve as a *something-you-have* authentication factor that need not be kept strictly in the possession of a user or uniquely assigned to a single individual. Tagged authentication objects can be shared by multiple individuals and provide an easy to use, low cost substitute for systems based on expensive, individually assigned tokens.

The end-to-end data integrity, origin authenticity, and confidentiality of biometric information and RFID tag data can be provided using efficient signcryption techniques. Signcryption can provide secure data transfer and storage for biometric reference templates, person-object associations, and for the sensitive information in authentication request and response messages.

References

1. International Organization for Standardization. ISO 19092 – Financial services – Biometrics – Security framework; 2008.
2. International Organization for Standardization / International Electrotechnical Commission. ISO/IEC 19785-1 Information technology – Common Biometric Exchange Formats Framework – Part 1: Data element specification; 2006.
3. Banks J, Pachano M, Thompson L, and Hanny D. RFID Applied. Hoboken, New Jersey: John Wiley & Sons, Inc; 2007.
4. X9 Financial Services. ANSI X9.117 Secure Remote Access – Mutual Authentication; 2012.
5. Griffin P. Biometric Authentication Objects For Access Control. Proceedings of the Future Security Research Conference, Future Security 2013, Berlin, Germany; 2013.
6. Griffin P. U.S. Patent Number 8,289,135. Washington, DC: United States; 2012.
7. Larmouth J. *ASN.1 complete*. San Francisco: Morgan Kaufmann Publishers; 2000.
8. Griffin P. Protecting Biometrics Using Signcryption. Proceedings of ID360: The Global Forum on Identity, the Center for Identity, University of Texas at Austin; 2012.
9. Bellare M, Namprempre C. Authenticated Encryption: Relations Among Notions and Analysis of the Generic Composition Paradigm. Journal of Cryptology; 2007; 21:4. p. 469-491.
10. Yavuz A, Alagöz F, Anarim E. A new multi-tier adaptive military MANET security protocol using hybrid cryptography and signcryption. Turkish Journal of Electrical Engineering & Computer Sciences; 2010; *18*:1. P. 1-21.
11. Griffin P. Telebiometric Security and Safety Management. Proceedings of ITU Kaleidoscope Conference – Building Sustainable Communities; 2013
12. Zheng Y. Shortened Digital Signature, Signcryption and Compact and Unforgeable Key Agreement Schemes; 1998.
13. Barbosa M, Farshim P. Certificateless signcryption. Asia CCS ’08; 2008.
14. Abdalla M, Camensich J, Canard S, Catalano D, Coron J, Courtois N, et al. New technical trends in asymmetric cryptography, ECRYPT (Network of Excellence in Cryptology), AZTEC Report; 2005.
15. Smith C. Digital signcryption; 2005.
16. Griffin P. Signcryption for biometric security. Journal of Cyber Security and Information Systems, 1(1); 2012.
17. Hu V, Schnitzer A, and Sandlin K. NIST Special Publication 800-162 Attribute Based Access Control Definition and Considerations, 2014.