ETSI TS 103 532 V1.2.1 (2021-05)

CYBER;
Attribute Based Encryption for Attribute Based Access Control

Reference

RTS/CYBER-0068

Keywords

access control, privacy

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Cyber Security (CYBER).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document specifies trust models, functions and protocols using attribute based encryption as a foundation of an attribute based access control scheme. It covers both the Ciphertext-Policy (CP-ABE) and Key-Policy (KP-ABE) variants of Attribute-Based Encryption.

The specifications address the following aspects:

- Identification of an ABE scheme covering both the Ciphertext-Policy and Key-Policy variants.
- Definition of interactions between the data sources, the service providers and the authority releasing attributes and key material.
- Mechanisms for keys, policies, and attributes distribution.
- Mechanisms for secret key expiration and revocation.
- Definition of semantics for a basic set of attributes to ensure interoperability.
- Mapping to a standard Public Key Infrastructure X.509.
- Mapping to a standard assertion protocol (SAML).
- Definition of a policy schema for data access control.
- Identification of limitations compared to traditional ABAC features.
- Translation rules to XACML.
- Definition of new protocol bindings when existing bindings do not cover the deployment scenario (e.g. a CoAP binding for the IoT case).

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference/.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

[1] Bureau international des poids et mesures: "The International System of Units (SI)".

[2] NIST SP 800-56B Revision 1: "Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography".

[3] Federal Information Processing Standards Publication (FIPS) 197: "Advanced Encryption Standard".

[4] IETF RFC 4648: "The Base16, Base32 and Base64 Data Encodings".

[5] OASIS: "Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0".

[6] OASIS: "Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0".

[7] OASIS: "XACML v3.0 Core and Hierarchical Role Based Access Control (RBAC) Profile Version 1.0".

[8] W3C Recommendation 28 October 2004: "XML Schema Part 2: Datatypes".

NOTE: Available at https://www.w3.org/TR/xmlschema-2/.

[9] OASIS: "eXtensible Access Control Markup Language (XACML) Version 3.0".

[10] ANSI INCITS 4-1986[R2017]: "Information Systems - Coded Character Sets - 7-Bit American National Standard Code for Information Interchange (7-Bit ASCII)".

[11] ISO/IEC 8601:2004: "Data elements and interchange formats - Information interchange - Representation of dates and times".

[12] W3C Recommendation 11 April 2013: "XML Encryption Syntax and Processing Version 1.1".

NOTE: Available at https://www.w3.org/TR/xmlenc-core1/.

[13] IETF RFC 5234: "Augmented BNF for Syntax Specifications: ABNF".

[14] ANSI/IEEE 754™-2008 :"IEEE Standard for Floating-Point Arithmetic".

[15] IETF RFC 7252: "The Constrained Application Protocol (CoAP)".

[16] IETF RFC 7959: "Block-Wise Transfer in the Constrained Application Protocol (CoAP)".

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ISO/IEC 29100:2011: "Information technology - Security techniques - Privacy framework".

[i.2] National Institute of Standards and Technology NIST SP 800-122: "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)".

[i.3] ETSI TS 103 458: "CYBER; Application of Attribute Based Encryption (ABE) for PII and personal data protection on IoT devices, WLAN, cloud and mobile services - High level requirements".

[i.4] ISO/IEC 18031:2011: "Information technology - Security techniques - Random bit generation".

[i.5] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[i.6] J. Bethencourt, A. Sahai, B. Waters: "Ciphertext-policy attribute-based encryption". Proceedings of the 2007 IEEE Symposium on Security and Privacy, SP'07, pages 321-334. Washington, DC, USA, 2007. IEEE Computer Society.

[i.7] ETSI TR 187 010: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Report on issues related to security in identity imanagement and their resolution in the NGN".

[i.8] ISO/IEC 17789:2014: "Information technology - Cloud computing - Reference architecture".

[i.9] ISO/IEC 19944:2017 "Information technology - Cloud computing - Cloud services and devices: Data flow, data categories and data use".

[i.10] ISO/IEC 17788: "Information technology - Cloud computing - Overview and vocabulary".

[i.11] Herranz, J., Laguillaumie, F. & Ràfols, C. (2010): "Constant Size Ciphertexts in Threshold Attribute-Based Encryption". Public Key Cryptography, (p. 19-34).

[i.12] N. Attrapadung, H. Imai: "Attribute-Based Encryption Supporting Direct/Indirect Revocation Modes". Proceedings of the 12th IMA International Conference on Cryptography and Coding. Pages 278 - 300. Cirencester, UK - December 15 - 17, 2009. Springer-Verlag.

[i.13] Ostrovsky, R., Sahai, A. & Waters, B. (2007): "Attribute-based encryption with non-monotonic access structures". ACM Conference on Computer and Communications Security, (p. 195-203).

[i.14] Attrapadung, N., Libert, B. & de Panafieu, E. (2011): "Expressive Key-Policy Attribute-Based Encryption with Constant-Size Ciphertexts". Public Key Cryptography, (p. 90-108).

[i.15] Lewko, A. B., Sahai, A. & Waters, B. (2010): "Revocation Systems with Very Small Private Keys". IEEE Symposium on Security and Privacy, (p. 273-285).

[i.16] ETSI TS 118 112: "oneM2M; Base Ontology (oneM2M TS-0012 version 2.2.2 Release 2A)".

[i.17] ISO/IEC 18033-1:2015: "Information technology - Security techniques - Encryption algorithms - Part 1: General".

[i.18] ISO/IEC 18033-5:2015: "Information technology - Security techniques - Encryption algorithms - Part 5: Identity based ciphers".

[i.19] ISO/IEC 24760-1:2011: "Information technology - Security techniques - A framework for identity management - Part 1: Terminology and concepts".

[i.20] Yannis Rouselakis, Brent Waters: "Efficient Statically-Secure Large-Universe Multi-Authority Attribute-Based Encryption". Financial Cryptography 2015: 315-332.

[i.21] IETF RFC 4119: "A Presence-based GEOPRIV Location Object Format".

[i.22] IETF RFC 2253: "Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names".

[i.23] IETF RFC 2821: "Simple Mail Transfer Protocol".

[i.24] IETF RFC 2732: "Format for Literal IPv6 Addresses in URL's".

[i.25] IETF RFC 2396: "Uniform Resource Identifiers (URI): Generic Syntax".

[i.26] W3C: "XML Path Language (XPath)".

NOTE: Available at https://www.w3.org/TR/xpath/.

[i.27] IETF RFC 3261: "SIP: Session Initiation Protocol".

[i.28] ISO/IEC 15946-1: "Information technology - Security techniques - Cryptographic techniques based on elliptic curves - Part 1: General".

[i.29] IETF RFC 822: "Standard for the Format of ARPA Internet Text Messages".

[i.30] Recommendation ITU-T X.520: "Information technology - Open Systems Interconnection - The Directory: Selected attribute types".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

ABE authority: ABE entity that stores the master secret key and gives out secret keys

ABKEM universe: set of attributes in which the number of attributes can be a linear (small-universe) or exponential (large-universe) function of the system's security strength

ABKEM universe regeneration: procedure by which an entirely new ABKEM universe is generated, with redistribution of new public key, new master secret key and new secret keys

app: "software application", typically running on a user's device platform

assertion: statement made by an authority about a property of an entity, typically for - but not restricted to - access control decisions

asymmetric encryption system: encryption system based on asymmetric cryptographic techniques whose public transformation is used for encryption and whose private transformation is used for decryption

NOTE: See ISO/IEC 18033-1 [i.17].

attack: algorithm that performs computations and makes queries to the encryption algorithm for the encryption and/or for the decryption of adaptively chosen texts under a single secret key, with the purpose of recovering either the unknown plaintext for a given ciphertext, which may be adaptively chosen but for which a decryption query is not issued or a secret key

NOTE: See ISO/IEC 18033-1 [i.17].

attack cost: ratio of the average complexity of the attack algorithm measured in terms of the number of calls to the encryption algorithm made by the attack to the probability of success of the attack

NOTE: See ISO/IEC 18033-1 [i.17].

attribute: characteristic or property of an entity that can be used to describe its state, appearance or other aspects

NOTE: See ISO/IEC 24760-1 [i.19].

Attribute-Based Encryption (ABE) system: asymmetric encryption system which is either a CP-ABE system, a KP-ABE system or a combination of both

attribute universe: set of attributes

cloud platform provider: cloud service provider providing identity management services and interfaces (e.g. API, marketplace, etc.) for third party applications using the platform services

cloud platform user: cloud service user consuming one or more platform services

cloud service customer: individual or organization consuming one or more cloud services provided by a cloud service provider

cloud service partner: individual or organization providing support to the provisioning of cloud services by the cloud service provider, or to the consumption of cloud service by the cloud service customer

cloud service provider: individual or organization providing cloud services to one or more cloud service customers

cloud service user: individual consuming one or more cloud services using a particular device

ciphertext: data which has been transformed to hide its information content

NOTE: See ISO/IEC 18033-1 [i.17].

Ciphertext-Policy Attribute-Based Encryption (CP-ABE) system: asymmetric encryption system where secret keys are derived from a set of attributes and ciphertexts are derived from a policy on attributes

data consumer: natural or legal person, public authority, agency or any other body accessing data for a given purpose

data controller: natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data

data processor: natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller

data subject: identifiable person, i.e. a person who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity

decryption: reversal of a corresponding encryption

NOTE: See ISO/IEC 18033-1 [i.17].

decryptor: entity which decrypts ciphertexts

NOTE: See ISO/IEC 18033-1 [i.17].

encryption: (reversible) transformation of data by a cryptographic algorithm to produce a ciphertext, i.e. to hide the information content of the data

NOTE: See ISO/IEC 18033-1 [i.17].

encryptor: entity which encrypts ciphertexts

NOTE: See ISO/IEC 18033-1 [i.17].

entity: item inside or outside an information and communication technology system, such as a person, an organization, a device, a subsystem or a group of such items that has recognizable distinct existence

NOTE: See ISO/IEC 24760-1 [i.19].

home network: central source for mobility services to the subscriber. The subscriber has a direct subscription with the home network

identity: set of attributes related to an entity

NOTE: See ISO/IEC 24760-1 [i.19].

Key-Policy Attribute-Based Encryption (KP-ABE) system: asymmetric encryption system where ciphertexts are derived from a set of attributes and secret keys are derived from a policy on attributes

match: policy statement in the access structure is said to match when the attributes in the annotation allow said statement to be evaluated to true in the logical sense

master public key: public value uniquely determined by the corresponding master secret key

NOTE: See ISO/IEC 18033-5 [i.18].

master secret key: secret value used by the secret key generator to compute secret keys for an ABE mechanism

personal data: any information relating to an identified or identifiable natural person ('data subject')

Personally Identifiable Information (PII): any information that:

a) can be used to identify the PII principal to whom such information relates; or

b) is or might be directly or indirectly linked to a PII principal.

NOTE 1: To determine whether a PII principal is identifiable, account can be taken of all the means which can reasonably be used by the privacy stakeholder holding the data, or by any other party, to identify that natural person (ISO/IEC 29100 [i.1]).

NOTE 2: In the US, according to NIST SP 800-122 [i.2], any information about an individual maintained by an agency, including any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

PII controller: privacy stakeholder that determines the purposes and means for processing personally identifiable information (PII) other than natural persons who use data for personal purposes

NOTE: See ISO/IEC 29100:2011 [i.1].

PII principal: natural person to whom the personally identifiable information (PII) relates

NOTE: See ISO/IEC 29100:2011 [i.1].

PII processor: privacy stakeholder that processes personally identifiable information (PII) on behalf of and in accordance with the instructions of a PII controller

NOTE: See ISO/IEC 29100:2011 [i.1].

plaintext: unencrypted information

NOTE: See ISO/IEC 18033-1 [i.17].

platform Provider: service provider providing services necessary to support a platform

secret key generator: entity or function which generates a set of secret keys

NOTE: See ISO/IEC 18033-5 [i.18].

policy on attributes: boolean predicate on attributes combining equality and/or inequality tests

policy statement: elementary test in an access control policy (e.g. "A < B")

processing of PII: operation or set of operations performed upon personally identifiable information (PII)

NOTE 1: See ISO/IEC 29100:2011 [i.1].

NOTE 2: Examples of processing operations of PII include, but are not limited to, the collection, storage, alteration, retrieval, consultation, disclosure, anonymization, pseudonymization, dissemination or otherwise making available, deletion or destruction of PII) [i.1].

random tape: source of (pseudo-)random bits

security strength: number associated with the amount of work (e.g. the number of operations) that is required to break a cryptographic algorithm or system

NOTE: See ISO/IEC 18033-1 [i.17].

serving network: home network or visited network the user equipment is connected to

set up: process by which the system parameters of an ABE mechanism are selected

set up algorithm: process which generates a master secret key and the corresponding master public key, together with some part of the system parameters

NOTE: See ISO/IEC 18033-5 [i.18].

setup party: entity that specifies the security parameter and handles the setup of the ABE and ABKEM system

subscriber User Equipment (UE): any device allowing a user access to network services

system parameters: parameters for cryptographic computation including a selection of a particular cryptographic scheme or function from a family of cryptographic schemes of functions, or from a family of mathematical spaces

NOTE: See ISO/IEC 18033-5 [i.18].

top-level policy statement: policy statement that is evaluated in all branches of the access structure

trust: level of confidence in the reliability and integrity of an entity to fulfil specific responsibilities

Trusted Authority (TA): ABE authority entitled to generate the public key PK and the corresponding secret keys according to a selected large universe ABE scheme

visited network: any network that interacts with the home network to provide mobility services to the subscriber terminal

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

3SP	Third Party Service Provider
AAD	Additional Authentic Data
ABAC	Attribute-Based Access Control
ABE	Attribute-Based Encryption
ABEA	Attribute-Based Encryption Authority
ABFN	Augmented Backus-Naur Form
ABKEM	Attribute-Based Key-Encapsulation Mechanism
ABNF	Augmented Backus-Naur Form
AE	Authenticated Encryption
AES	Advanced Encryption Standard
AP	Access Policy
API	Application Programming Interface
ASCII	American Standard Code for Information Interchange
BDH	Bilinear Diffie-Hellman
CA	Certification Authority
C_{AE}	Ciphertext for Authenticated Encryption
CCA	Chosen-Ciphertext Attack
CP	Ciphertext Policy
CPA	Chosen-Plaintext Attack
CP-ABE	Ciphertext Policy ABE
CP-ABKEM	Ciphertext Policy ABKEM
CRL	Certificate Revocation List
DBDDH	Decisional Bilinear DDH
DBDHE	Decisional Bilinear Diffie-Hellman Exponent
DDH	Decisional Diffie-Hellman
DNS	Domain Name System
DPP	Device Platform Provider
ECDSA	Elliptic Curve Digital Signature Algorithm
GGM	Generic Group Model
GML	Geography Markup Language
IBBE	Identity-Based Broadcast Encryption
IP	Internet Protocol
K_{AE}	Symmetric Key for Authenticated Encryption
KEM	Key Encapsulation Mechanism
KP	Key-Policy
KP-ABE	Key Policy ABE
KP-ABKEM	Key Policy ABKEM
LO	IETF GeoPriv Location Object
MEBDH	Multi-Exponent BDH
MPK	Master Public Key
MSK	Master Secret Key
MSP	Monoton Span Program
NIST	National Institute of Standards and Technology
OR	OR (bitwise operator)