ETSI TS 103 458 V1.1.1 (2018-06)

CYBER;
Application of Attribute Based Encryption (ABE) for PII and personal data protection on IoT devices, WLAN, cloud and mobile services - High level requirements

Reference
DTS/CYBER-0020

Keywords
access control, confidentiality, portability, 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 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is 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 IPR Policy, no investigation, 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.

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 high level requirements for the application of Attribute Based Encryption (ABE) to protect PII and personal data on IoT devices/services, cloud services, Wireless Local Area Networks and mobile services, where access to data has to be given to multiple parties and under different conditions. With a main focus on the confidentiality of data, including personal data and Personally Identifiable Information, the present document may help in supporting the General Data Protection Regulation [i.19].

The following use cases are described:

1) The Mobile use case describes a situation of user access from less trusted networks. The objective is to provide user identity protection preserving disclosure to unauthorized entity.

2) The federated WLAN use case where users can access different WLAN networks using their credentials - issued by different authorities/domains - while preserving their privacy.

3) Many Internet of Things use cases or edge scenarios where data access mechanisms are actioned either in the network or on the device.

4) The Cloud use case where a third party accesses personal data from the Cloud Service Provider.

The present document also provides recommendations on the ABE scheme to use for each use 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.

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

2.2 Informative references

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. For non-specific references, the latest version of the referenced document (including any amendments) applies.

[i.1] Italian Digital Agency: "Three-Year Plan for ICT in Public Administration (2017 - 2019)".

NOTE: Available at https://pianotriennale-ict.readthedocs.io/en/latest/.

[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 133 401: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 3GPP System Architecture Evolution (SAE); Security architecture (3GPP TS 33.401)".

[i.4] 3GPP TR 22.864: "Feasibility study on new services and markets technology enablers for network operation; Stage 1".

[i.5] ISO/IEC 19944:2017: "Information technology - Cloud computing - Cloud services and devices: Data flow, data categories and data use".

[i.6] FP7-ICT 611659 AU2EU Deliverable D4.2.1: "Cryptographically enforced access control".

NOTE: Available at http://www.au2eu.eu/uploads/Publications/deliverables/AU2EU_D4.2.2_Final.pdf.

[i.7] 5G Ensure project: "Deliverable D2.1: Use Cases".

NOTE: Available at http://www.5gensure.eu/sites/default/files/Deliverables/5G-ENSURE_D2.1-UseCases.pdf.

[i.8] F. van den Broek, R. Verdult, J. de Ruiter: "Defeating IMSI Catchers".

NOTE: Available at http://www.cs.ru.nl/~rverdult/Defeating_IMSI_Catchers-CCS_2015.pdf.

[i.9] P. Paillier: "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes", EUROCRYPT, pages 223-238. Springer, 1999.

NOTE: Available at https://link.springer.com/chapter/10.1007/3-540-48910-X_16.

[i.10] ETSI TR 101 567: "Lawful Interception (LI); Cloud/Virtual Services for Lawful Interception (LI) and Retained Data (RD)".

[i.11] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, W. Jonker: "Information security applications", pages 309-323, Springer-Verlag, Berlin, Heidelberg, 2009.

[i.12] A. Sahai, B. Waters: "Fuzzy Identity Based Encryption", Advances in Cryptology - EUROCRYPT, Volume 3494 of LNCS, pages 457-473. Springer, 2005.

[i.13] V. Goyal, O. Pandey, A. Sahai, B. Waters: "Attribute-based encryption for fine-grained access control of encrypted data", Proceedings of the 13th ACM Conference on Computer and Communications Security, CCS '06, pages 8-98, New York, NY, USA, 2006. ACM.

[i.14] J. Bethencourt, A. Sahai, B. Waters: "Ciphertext-policy attribute-based encryption", Proceedings of the 2007 IEEE Symposium on Security and Privacy, SP'07, pages 32-334. Washington, DC, USA, IEEE Computer Society.

[i.15] A. Boldyreva, V. Goyal, V. Kumar: "Identity based encryption with efficient revocation", Conference on Computer and Communications Security, pages 417-416, 2008.

[i.16] 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.17] M. Piretti, P. Traynor, P. McDaniel, B. Waters: "Secure attribute-based systems", Journal of Computer Security, 18(5), pages 799-837, 2010.

[i.18] Z. Xu, K. Martin: "Dynamic User Revocation and Key Refreshing for Attribute-Based Encryption in Cloud Storage", Trust, Security and Privacy in Computing and Communications (TrustCom), IEEE 11th International Conference, 2012, pp. 844-849.

[i.19] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[i.20] ISO/IEC 29100:2011: "Information technology - Security techniques - Privacy framework".

[i.21] ETSI TS 103 532: "CYBER; Attribute Based Encryption for Attribute Based Access Control".

[i.22] Directive 2012/18/EU of the European Parliament and of the Council of 4 July 2012 on the control of major-accident hazards involving dangerous substances, amending and subsequently repealing Council Directive 96/82/EC Text with EEA relevance.

[i.23] IEEE 802.11: "IEEE Standard for Information technology--Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," in IEEE Std 802.11-2016 (Revision of IEEE Std 802.11-2012) , vol., no., pp.1-3534, Dec. 14 2016.

3 Definitions and abbreviations

3.1 Definitions

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

cloud platform provider: cloud service provider providing identity management services and interfaces 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

data subject: identified or identifiable natural person to which the data relates, or device that produces data that can be linked to a natural person

NOTE: In the sense of the GDPR [i.19], an identified or identifiable natural person to which the data relates. In the present document, this definition is extended to devices that produce data that can be linked to a natural person. See also PII principal.

direct access: access to data that is available in cleartext via a software-based access control system

generated data: data that is the result of an analytical process performed on behalf of, and which still relate to, the data subject

NOTE 1: Typically, generated data can be the result of a process applied to operational data.

NOTE 2: Depending on their characteristics, generated data can fall into the category of personal data as defined by the GDPR [i.19].

home network: central source for mobility services to the subscriber

NOTE: The subscriber has a direct subscription with the Home Network.

indirect access: access to data that is available in ciphertext form and requires the separate provisioning of a key followed by a decryption step, before the data can be accessed

key management: administration and use of the generation, registration, certification, deregistration, distribution, installation, storage, archiving, revocation, derivation and destruction of keying material in accordance with a security policy

location data: data composed of a position and a timestamp.

lone worker: employee who performs an activity that is carried out in isolation from other workers without close or direct supervision

operational data: data that is captured by a device on behalf of the data subject

NOTE 1: In an industrial context, this includes data captured by the worker's equipment as well as by facilities provided by the workplace (e.g. the physical access control system of a restricted area).

NOTE 2: Depending on their characteristics, operational data can fall into the category of personal data as defined by the GDPR [i.19].

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 [i.20].

NOTE 2: In the US, according to [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 [i.20]

PII principal: natural person to whom the personally identifiable information (PII) relates [i.20]

PII processor: privacy stakeholder that processes personally identifiable information (PII) on behalf of and in accordance with the instructions of a PII controller [i.20]

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

processing of PII: operation or set of operations performed upon personally identifiable information (PII) [i.20]

NOTE: 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.20].

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

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

static data: data that has been configured by the owner (e.g. an employee) on their devices, or by the device manager (e.g. the employer) on behalf of the owner

NOTE: Depending on their characteristics, Static Data can fall into the category of personal data as defined by the GDPR [i.19].

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 master public key MPK and the corresponding secret keys according to a selected large universe ABE scheme

NOTE: A Trusted Authority can be implemented as a Key Management Server (KMS) and can be distributed across several servers residing on different domains.

untrusted storage: memory storage that is not trusted to provide adequate confidentiality and access control guarantees for the stored data

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

3.2 Abbreviations

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

2G	2nd Generation (mobile networks)
3G	3nd Generation (mobile networks)
4G	4nd Generation (mobile networks) also known as LTE

5G	5nd Generation (mobile networks)
ABAC	Attribute Based Access Control
ABE	Attribute Based Encryption
AKA	Authentication Key Agreement
ANPR	Anagrafe Nazionale della Popolazione Residente
AP	Access Point
API	Application Programming Interface
AV	Authentication Vector
CA	Certification Authority
CP-ABE	Ciphertext Policy Attribute Based Encryption
CPU	Central Processing Unit
CSPa	Cloud Service Partner
CT	CipherText
EU	European Union
GDPR	General Data Protection Regulation
GUTI	Globally Unique Temporary Identifier
IA	Issuing Authority
ICT	Information and Communication Technology
IMEI	International Mobile Station Equipment Identity
IMSI	International Mobile Subscriber Identity
IoT	Internet of Things
KMS	Key Management Server
KP-ABE	Key Policy Attribute Based Encryption
LEA	Law Enforcement Authority
LI	Lawful Interception
LTE	Long Term Evolution
MAC	Medium Access Control
MCC	Mobile Country Code
MME	Mobility Management Entity
MNC	Mobile Network Code
MNO	Mobile Network Operator
MPK	Master Public Key
MSIN	Mobile Subscription Identification Number
MSK	Master Secret Key
OTA	Over The Air
PII	Personally Identifiable Information
PK	Public Key
PKI	Public Key Infrastructure
PLMN	Public Land Mobile Network
PLMN-id	Public Land Mobile Network Identifier
PP	Platform Provider
PSK	Pre-Shared Secret
Pu	Platform user
RADIUS	Remote Authentication Dial-In User Service
SAML	Security Assertion Markup Language
SIM	Subscriber Identity Module
SK	Secret Key
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SP	Service Provider
SR	Service Requestor
STA	Station
TA	Trusted Authority
TR	Technical Report
UE	User Equipment
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WM	WLAN Manager
WP	WLAN Provider
WPA	Wi-Fi Protected Access

4 Mobile use case

4.1 Introduction

4.1.1 Scenario

This solution presents an alternative mechanism to conceal permanent or long-term subscription identifier when a temporary subscription identifier is not available (c.f. initial Attach Request in LTE). Information provided over the air during initial attach request in LTE can allow a passive eavesdropper to obtain a variety of sensitive information including, but not limit to: user identity, user subscribed services such as voice, messaging, data et cetera, location information, traffic, network usage [i.4].

By design, current mobile networks need to occasionally expose long terms identities such as IMSI or IMEI, but in some circumstances (e.g. before network attach is complete), no protection can be offered in all current systems. This is because mobile telecommunication systems (e.g. 2G, 3G, 4G) mandate the use of symmetric-key cryptography schemes, with pre-shared secret key, for guaranteeing user/network authentication and confidentiality and integrity of data sent over the air. Such schemes are based on the assumption that the user has been previously identified by the network. In the AKA method (Authentication Key Agreement) [i.3] the user is required to first provide his/her subscriber identifier (i.e. the IMSI - International Mobile Subscriber Identity) in order for the mobile network to be able to subsequently retrieve the user's credentials (including the user-specific pre-shared secret key) and perform the user authentication procedure. The subscriber identifier is sent to the mobile network in clear text, since initially no cryptographic material is yet available/shared between the user and the network before the conclusion of the AKA procedure.

EXAMPLE: John is visiting a foreign country and switches on his mobile. The visited PLMN requests John's user identity (e.g. the IMSI) in order to authenticate him. John implicitly relies on the assumption that the visited PLMN is a trusted network. Unauthorized disclosure of sensitive PII can happen if interconnected networks are not "legitimate" as expected to be [i.7].

The lack of protection can lead to users' privacy breaches such as the disclosure of subscription identifier to an unauthorized party, the subscriber spoofing, and the detection of subscriber's presence in certain location. An attacker can gather, for example by means of an IMSI sniffer, all IMSIs that are active in a certain geographic area. An IMSI sniffer can achieve this in two different manners: passive and active. A passive sniffer will be simply observing unencrypted wireless traffic and storing all observed IMSIs. An active sniffer will be using a fake base station (fake BTS - Base Transceiver Station), to which mobile phones (UE) in the neighbourhood will attempt to connect due to the detection of a stronger radio signal, and the fake base station will request (e.g. with an Identity Request message) each UE to identify itself. The active IMSI sniffing is also known as IMSI catching in the mobile networks environment, and it is considered a feasible attack and, in recent years, even affordable by using out-of-the-shelves tools.

IMSI sniffing/catching attacks mostly relate to the issue of users' location privacy, as the transmission of IMSI reveals the user approximate location. Location privacy attacks attempt to link an identity to a location. User's location tracking is performed by sniffing the user identities sent in clear text over the air. An attacker can collect users' identities in an area or place (e.g. in an airport) and can further on track the users' presence and movements.

The information can also be used to impersonate the user or to cause denial of service.

4.1.2 Preliminary considerations

A major problem in current mobile networks is that identifiers are occasionally exposed in situations where no security context (i.e. shared cryptographic material) is available, neither to authenticate identity requests, nor to protect (encrypt) the IMSI in the identity response, as well as in attach request messages, thus enabling UEs tracking.

The security problem is briefly summarized below:

- The IMSI is transmitted in clear text in the first Attach Request.
- Identity Requests are not authenticated and are used to retrieve the long-term user identity, e.g. in the case when the temporary identity (e.g. GUTI in 4G) results as invalid. This implies that the user's Identity Response contains the IMSI in clear text.

- Encryption of signalling is required to transmit subscriber's identities in a protected way. However, availability of encryption depends on the network configuration.

Temporary identities reallocation depends entirely on operator configuration. This situation can be exploited by attackers as described in the literature [i.8].

In comparison with symmetric-key cryptography method like AKA [i.3], the use of asymmetric-key (or public-key) cryptography can provide an increased level of protection of sensitive data exchange during user identification. In principle, to initiate the network Attach procedure, the subscriber's identity could be encrypted using the public key of the network operator. This way, the UE would not need to send its identity in the clear.

In particular, public-key encryption can be needed in the following situations:

- Attach Request - contains IMSI in clear text: the IMSI (and maybe other sensitive information, e.g. network and security capability) should be encrypted with the public key of the serving/home network (the public key is stored on the SIM, while the private key is available on the 5G Mobile Management Entity (MME)). Randomized encryption schemes should be applied in order to prevent linkability. Therefore, the risk that IMSI catchers can read, guess or track the IMSI is reduced.

- Identity Response - contains IMSI in clear text: the IMSI should be encrypted with the public key of the network (the public key is stored on the SIM, while the private key is available on the 5G MME). Randomized encryption schemes can be applied, such as homomorphic cryptosystems (e.g. [i.9]) or ABE encryption schemes. Therefore the risk that IMSI catchers can read or guess the IMSI is reduced.

If traditional public-key encryption were used to avoid an unauthorized disclosure of its identity, the UE would have to use the public key of the visited serving network. This would be impractical, as the UE would have to be securely provisioned with all public keys (more precisely, with unexpired public-key certificates or certificate chains with trusted public keys in the corresponding digital signatures) of all possible networks it can roam into and select the one to use based on the PLMN (Public Land Mobile Network) identifier. A public-key certificate signed by an authority binds a public key to an identity (e.g. a network identity). Public Key Infrastructure (PKI) is needed to generate and manage the required public-key certificates and the public keys used for signing the certificates need to be all trusted.

The present clause is intended to tackle this problem using a technique based on attribute based encryption. To this end, the following high level requirements are defined.

4.2 High level requirements

The present document specifies the following high level requirements (table 4.1) for the Mobile use case.