ETSI TR 103 618 V1.1.1 (2019-12)

TECHNICAL REPORT

CYBER;
Quantum-Safe Identity-Based Encryption

Reference
DTR/CYBER-QSC-0012

Keywords
encryption, identity, security

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/057e4fb-cecc-4a62-8a87-e7f3e1606bd/etsi-tr-103-618-v1.1.1-2019-12

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

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.
The content of the PDF version shall not be modified without the written authorization of ETSI.
The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2019.
All rights reserved.

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.

Contents

Intellectual Property Rights 5
Foreword 5
Modal verbs terminology 5
1 Scope 6
2 References 6
2.1 Normative references 6
2.2 Informative references 6
3 Definition of terms, symbols and abbreviations 8
3.1 Terms 8
3.2 Symbols 9
3.3 Abbreviations 9
4 Identity-Based Encryption (IBE) 10
4.1 Introduction 10
4.2 Functionality 10
4.3 Discussion 12
4.4 Example use cases 13
4.5 Quantum-safe IBE 13
5 Lattice-based HIBE 14
5.1 Background 14
5.2 Overview 14
5.2.1 Polynomial ring 14
5.2.2 Central KMS lattice 15
5.2.3 Sub-KMS lattice 15
5.2.4 User lattice 16
5.2.5 Encryption 16
5.2.6 Validation 16
5.3 Parameters 16
5.4 Key generation 17
5.5 Delegation 18
5.6 Extraction 20
5.7 Message encoding 21
5.8 Encryption 21
5.9 Decryption 22
6 Parameter selection 23
6.1 Gaussian distributions 23
6.2 Ring dimension and modulus 23
6.3 Parameter sets 24
6.3.1 Single-level IBE scheme 24
6.3.2 Two-level HIBE scheme 24
6.3.3 Discussion 25
6.3.3.1 Master public key size 25
6.3.3.2 Gram-Schmidt storage 25
6.3.3.3 User private key size 25
6.3.3.4 Ciphertext sizes 26
6.4 Security estimates 26
7 Performance estimates 26
7.1 Performance on a 64-bit desktop processor 26
7.2 Performance on a 32-bit embedded processor 27
7.3 Discussion 28
7.3.1 Key generation 28
7.3.2 Extraction 28
7.3.3 Delegation 28

7.3.4 Encryption and decryption 28
8 Conclusion 29

Annex A: Mathematical background 30

A.1 Lattices 30
A.1.1 Bases and determinant 30
A.1.2 Gram-Schmidt 30
A.1.3 Nearest plane algorithm 30

A.2 Lattice-basis reduction 31
A.2.1 Gaussian heuristic 31
A.2.2 Estimating quality 31
A.2.3 Estimating lattice-basis cost 31

A.3 Sampling 32
A.3.1 Discrete Gaussians 32
A.3.2 Klein sampler 32

A.4 NTRU-style lattices 32
A.4.1 Isometric lattices 32
A.4.2 Isometric Gram-Schmidt 33
A.4.3 Isometric Klein sampler 33
A.4.4 Block isometric Gram-Schmidt 34
A.4.5 Block isometric Klein sampler 34

Annex B: Implementation considerations 35

B.1 Ciphertext compression 35

B.2 Number-Theoretic Transform 35

Annex C: Security considerations 37

C.1 Provable security 37
C.1.1 Security definitions 37
C.1.2 Bonsai scheme 37
C.1.3 LATTE 38
C.1.4 Active security 39

C.2 Practical security 39
C.2.1 Statistical security 39
C.2.2 Decryption failure 39
C.2.3 Master key recovery 40
C.2.4 Delegated key recovery 41
C.2.5 User key recovery 41
C.2.6 Message recovery 42

History 44

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 Report (TR) has been produced by ETSI Technical Committee Cyber Security (CYBER).

Modal verbs terminology

In the present document "**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 describes a proposal for a quantum-safe hierarchical identity-based encryption scheme. It gives an overview of the functionality provided by hierarchical identity-based encryption, outlines some example uses cases and provides a high-level description of a potential solution based on structured lattices. The description includes concrete proposals for parameter sets, estimates for performance in software and a practical security analysis.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

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] A. Shamir: "Identity-based cryptosystems and signature schemes", CRYPTO, 1984.

[i.2] J. Bethencourt, A. Sahai and B. Waters: "Ciphertext-Policy Attribute-Based Encryption", Security and Privacy, 2007.

[i.3] C. Gentry and A. Silverberg: "Hierarchical ID-Based Cryptography", ASIACRYPT, 2001.

[i.4] D. Boneh and M. Franklin: "Identity-Based Encryption from the Weil Pairing", CRYPTO, 2001.

[i.5] A. Boldyreva, V. Goyal and V. Kumar: "Identity-based Encryption with Efficient Revocation", CCS, 2008.

[i.6] J. H. Seo and K. Emura: "Revocable Identity-Based Encryption Revisited: Security Model and Construction", PKC, 2013.

[i.7] X. Ding and G. Tsudik: "Simple Identity-Based Cryptography with Mediated RSA", CT-RSA, 2003.

[i.8] K. Paterson and G. Price: "A comparison between traditional public key infrastructures and identity-based cryptography", Information Security Technical Report 8(3), 57-72, 2003.

[i.9] P. Szczechowiak and M. Collier: "TinyIBE: Identity-based encryption for heterogeneous sensor networks", Intelligent Sensors, Sensor Networks and Information Processing, 2009.

[i.10] ETSI EN 300 392-7: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security".

[i.11] ETSI EN 300 396-6: "Terrestrial Trunked Radio (TETRA); Direct Mode Operation (DMO); Part 6: Security".

[i.12] SAFEcrypto: "D9.1 - Case study specifications and requirements", June 2015.

NOTE: Available at https://www.safecrypto.eu/outcomes/deliverables.

[i.13] C. Cocks: "An identity based encryption scheme based on quadratic residues", IMA International Conference on Cryptography and Coding, 2001.

[i.14] C. Gentry, C. Peikert and V. Vaikuntanathan: "How to Use a Short Basis: Trapdoors for Hard Lattices and New Cryptographic Constructions", STOC, 2008.

[i.15] D. Cash, D. Hofheinz, E. Kiltz, C. Peikert: "Bonsai trees, or how to delegate a lattice basis", J. Cryptology 25(4), 601-639, 2012.

[i.16] S. Agrawal, D. Boneh and X. Boyen: "Efficient lattice (H)IBE in the standard model", EUROCRYPT, 2010.

[i.17] S. Agrawal, D. Boneh and X. Boyen: "Lattice basis delegation in fixed dimension and shorter-ciphertext hierarchical IBE", CRYPTO, 2010.

[i.18] L. Ducas, V. Lyubashevsky and T. Prest: "Efficient identity-based encryption over NTRU lattices", ASIACRYPT, 2014.

[i.19] P. Bert, P.-A. Fouque, A. Roux-Langlois and M. Sabt: "Practical implementation of Ring-SIS/LWE based signature and IBE", Post-Quantum Cryptography, 2018.

[i.20] S. McCarthy, N. Smyth and E. O'Sullivan: "A practical implementation of identity-based encryption over NTRU lattices", IMA International Conference on Cryptography and Coding, 2017.

[i.21] T. Güneysu and T. Oder: "Towards lightweight identity-based encryption for the post-quantum-secure Internet of Things", Quality Electronic Design, 2017.

[i.22] P. Klein: "Finding the closest lattice vector when it's unusually close", SODA, 2000.

[i.23] P. Q. Nguyen and O. Regev: "Learning a parallelepiped: Cryptanalysis of GGH and NTRU signatures", EUROCRYPT, 2006.

[i.24] D. Micciancio and S. Goldwasser: "Complexity of lattice problems: A cryptographic perspective", Kluwer Academic Publishers, Boston, 2002.

[i.25] V. Lyubashevsky, C. Peikert and O. Regev: "A Toolkit for Ring-LWE Cryptography", EUROCRYPT, 2013.

[i.26] P. Campbell and M. Groves: "Practical post-quantum Hierarchical Identity-Based Encryption", IMA Conference on Cryptography and Coding, 2017.

[i.27] S. Fluhrer: "Cryptanalysis of Ring-LWE based key exchange with key share reuse", IACR ePrint Archive 2016/085, 2016.

[i.28] E. Fujisaki and T. Okamoto: "Secure integration of asymmetric and symmetric encryption schemes", CRYPTO, 1999.

[i.29] T. Pöppelmann and T. Güneysu: "Towards practical lattice-based public-key encryption on reconfigurable hardware", SAC, 2013.

[i.30] M. Abe, R. Gennaro, K. Kurosawa and V. Shoup: "Tag-KEM/DEM: A new framework for hybrid encryption and a new analysis of Kurosawa-Desmedt KEM", EUROCRYPT, 2005.

[i.31] E. Alkim, R. Avanzi, J. Bos, L. Ducas, A. de la Piedra, T. Pöppelmann, P. Schwabe and D. Stebila: "NewHope: Algorithm specifications and supporting documentation", NIST First Round Post-Quantum Submission, 2017.

[i.32] V. Lyubashevsky and T. Prest: "Quadratic time, linear space algorithms for Gram-Schmidt orthogonalization and Gaussian sampling in structured lattices", EUROCRYPT, 2015.

[i.33] SAFEcrypto: "WP6: libsafecrypto".

NOTE: Available at https://www.github.com/safecrypto/libsafecrypto.

[i.34] T. Pornin and T. Prest: "More efficient algorithms for the NTRU key generation using the field norm", PKC, 2019.

[i.35] L. Ducas and T. Prest: "Fast Fourier orthogonalization", ISSAC, 2016.

[i.36] D. Stebila and M. Mosca: "Post-Quantum Key Exchange for the Internet and the Open Quantum Safe Project", SAC, 2016.

NOTE: Available at https://www.github.com/open-quantum-safe/liboqs.

[i.37] M. Albrecht, F. Göpfert, F. Virdia and T. Wunderer: "Revisiting the expected cost of solving uSVP and applications to LWE", ASIACRYPT, 2017.

[i.38] A. Becker, L. Ducas, N. Gama and T. Laarhoven: "New directions in nearest neighbor searching with applications to lattice sieving", SODA, 2016.

[i.39] M. Albrecht, Y. Lindell, E. Orsini, V. Osheter, K. Paterson, G. Peer and N. Smart: "LIMA: A PQC encryption scheme", NIST First Round Post-Quantum Submission, 2017.

[i.40] T. Laarhoven: "Search problems in cryptography: From fingerprinting to lattice sieving", PhD thesis, Eindhoven University of Technology, 2015.

[i.41] C. Peikert: "How (not) to instantiate Ring-LWE", SCN, 2016.

[i.42] V. Lyubashevsky C. Peikert and O. Regev: "On ideal lattices and learning with errors over rings", EUROCRYPT, 2010.

[i.43] M.-J. Saarinen: "Ring-LWE ciphertext compression and error correction: Tools of lightweight post-quantum cryptography", IoTPTS, 2017.

[i.44] P. Longa and M. Naehrig: "Speeding up the Number Theoretic Transform for faster ideal lattice-based cryptography", CANS, 2016.

[i.45] C. Peikert: "Lattice cryptography for the internet", Post-Quantum Cryptography, 2014.

[i.46] J.-P. D'Anvers, F. Vercauteren and I. Verbauwhede: "On the impact of decryption failures on the security of LWE/LWR based schemes", IACR ePrint Archive 2018/1089, 2018.

[i.47] E. Alkim, L. Ducas, T. Pöppelmann and P. Schwabe: "Post-quantum key exchange - a new hope", USENIX Security, 2016.

[i.48] P.-A. Fouque, J. Hoffstein, P. Kirchner, V. Lyubashevsky, T. Pornin, T. Prest, T. Ricosset, G. Seiler, W. Whyte and Z. Zhang: "FALCON: Fast-Fourier lattice-based compact signatures over NTRU", NIST First Round Post-Quantum Submission, 2017.

[i.49] P. Kirchner and P.-A. Fouque: "Revisiting lattice attacks on overstretched NTRU parameters", EUROCRYPT, 2017.

[i.50] J. Buchmann, F. Göpfert, R. Player and T. Wunderer: "On the Hardness of LWE with Binary Error: Revisiting the Hybrid Lattice-Reduction and Meet-in-the-Middle Attack", AFRICACRYPT, 2016.

3 Definition of terms, symbols and abbreviations

3.1 Terms

Void.

3.2 Symbols

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

$\bar{a}$	Transpose of the polynomial a
(a)	Vector of coefficients of the polynomial a
$\lfloor a \rceil$	Co-ordinatewise rounding of the polynomial a
$\|a\|$	Euclidean norm of the vector a
$a \cdot b$	Multiplication of the polynomials a and b
$a * b$	Co-ordinatewise multiplication of the vectors a and b
$a \,\|\|\, b$	Concatenation of the strings a and b
$a \oplus b$	Exclusive or of the values a and b
$\mathrm{Adv}(\mathcal{A})$	Advantage of the adversary $\mathcal{A}$
$\mathcal{B}^*$	Gram-Schmidt vectors corresponding to the basis $\mathcal{B}$
$\|\mathcal{B}\|_{GS}$	Gram-Schmidt norm of the basis $\mathcal{B}$
$D(\mu, \sigma)$	Discrete Gaussian distribution with mean μ and standard deviation σ
Γ	Gamma function
$\mathcal{M}(a)$	Matrix representation of the polynomial a
$\mathbb{Q}$	Rational numbers
$\mathbb{R}$	Real numbers
$\mathrm{Res}(a, b)$	Resultant of the polynomials a and b
$\mathbb{Z}$	Integers

3.3 Abbreviations

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

ABB	Agrawal, Boneh and Boyen
ABE	Attribute-Based Encryption
AMD	Advanced Micro Devices
AVX	Advanced Vector eXtensions
BKZ	Block Korkine-Zolotarev
CA	Certificate Authority
CCA	Chosen-Ciphertext Attack
CPA	Chosen-Plaintext Attack
CRL	Certificate Revocation List
DLP	Ducas, Lyubashevsky and Prest
GPV	Gentry, Peikert and Vaikuntanathan
HIBE	Hierarchical Identity-Based Encryption
IBE	Identity-Based Encryption
IND	INDistinguishability
IP	Internet Protocol
KDF	Key Derivation Function
KEM	Key Encapsulation Mechanism
KMS	Key Management Service
LWE	Learning With Errors
NIST	National Institute of Standards and Technology
NTT	Number-Theoretic Transform
OCSP	Online Certificate Status Protocol
PKI	Public-Key Infrastructure
QSC	Quantum-Safe Cryptography
SEM	SEcurity Mediator
TETRA	TErrestrial Trunked RAdio
URL	Universal Resource Locator

4 Identity-Based Encryption (IBE)

4.1 Introduction

In public-key cryptography each user has a key pair consisting of matched public and private keys.

Traditionally, the private key is generated first via a random process and the public key is derived from the private key via a mathematical function that is hard to invert. Public keys constructed in this way are pseudo-random and have no intrinsic meaning. Consequently, it is usually necessary to bind the public key to a public identifier associated to the user; e.g. the user's e-mail address, their device's Internet Protocol (IP) address or their website's Universal Resource Locator (URL). The binding is typically achieved by including the public key and identifier in a certificate that is digitally signed by a trusted third party such as a Certification Authority (CA) during a certification process.

In contrast, with identity-based cryptography [i.1] the public key is chosen first and the private key is derived from the public key. This means that a user's public key can have some intrinsic semantic value. Specifically, it can be chosen to be the representation of a public identifier associated with the user. The most important difference between traditional public-key cryptography and identity-based cryptography is that the user's private key needs to be derived from their identifier by a trusted third party such as a Key Management Service (KMS) during a registration process.

More generally, the public keys can include auxiliary information the user such as their employment status, authorizations or geographical location. This allows finer-grained access control as the KMS can verify that the user holds the appropriate authorizations before issuing the corresponding private key. A more flexible version of this functionality is provided by attribute-based cryptography [i.2] where, for example, data can be protected in such a way that only users whose attributes satisfy a certain policy are able to access it.

4.2 Functionality

One of the main advantages of identity-based cryptography is that it offers the possibility of lightweight key management without the need for certificates or a full public-key infrastructure (PKI).

If Alice wants to send Bob a message protected by a public-key encryption scheme where the public keys are managed by a PKI, then she first needs to obtain the certificate containing Bob's public key either directly from Bob or from a central certificate repository (Figure 1).

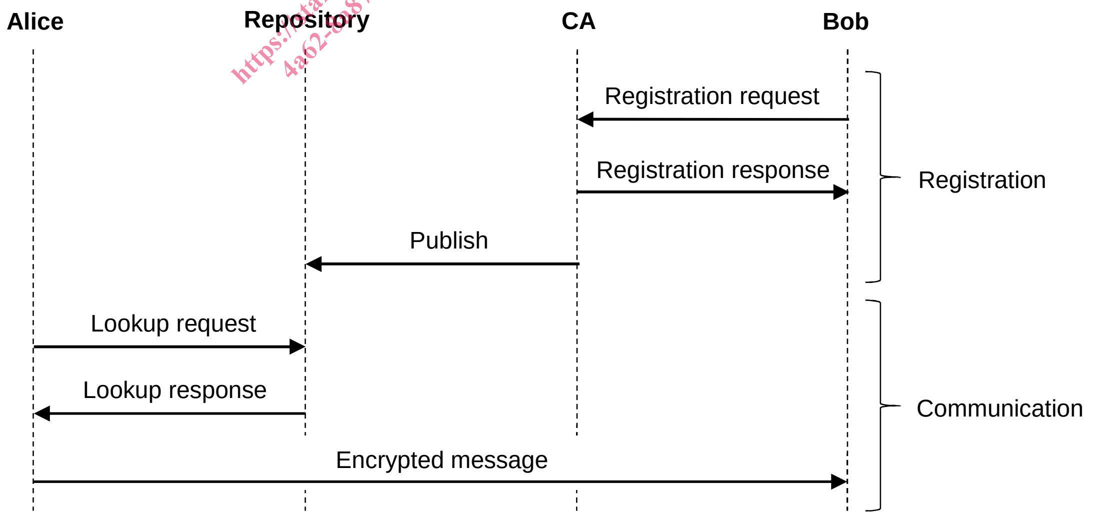

Figure 1: Encrypted communication with a PKI

If Alice wants to send Bob a message protected by an identity-based encryption (IBE) scheme, then she only needs to know Bob's public identifier as this corresponds to his authenticated public key. This can enable simplex transmission of encrypted messages without the involvement of the KMS (Figure 2). It is even possible for Alice to send Bob an encrypted message before he has registered and been given his private key.

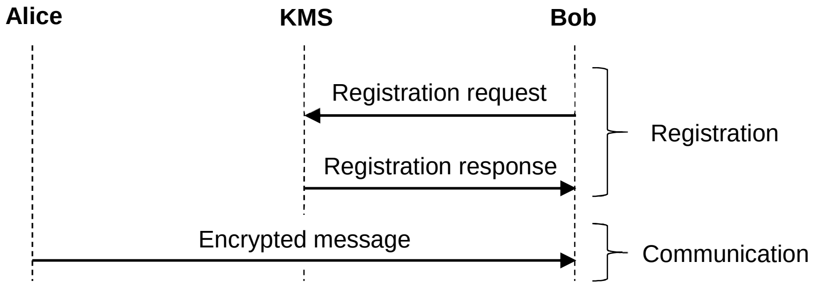

Figure 2: Encrypted communication with IBE

PKIs that handle a large number of users typically involve multiple levels of CAs. For example, in a two-tier model the root CA delegates authority to one or more issuing CAs who then sign the certificates containing user public keys. Hierarchical identity-based encryption (HIBE) [i.3] is an analogous concept. A central KMS delegates the ability to derive user private keys to one or more a sub-KMSs. This provides more scalable and flexible user management, and still allows simplex transmission of encrypted messages without the involvement of a KMS (Figure 3).

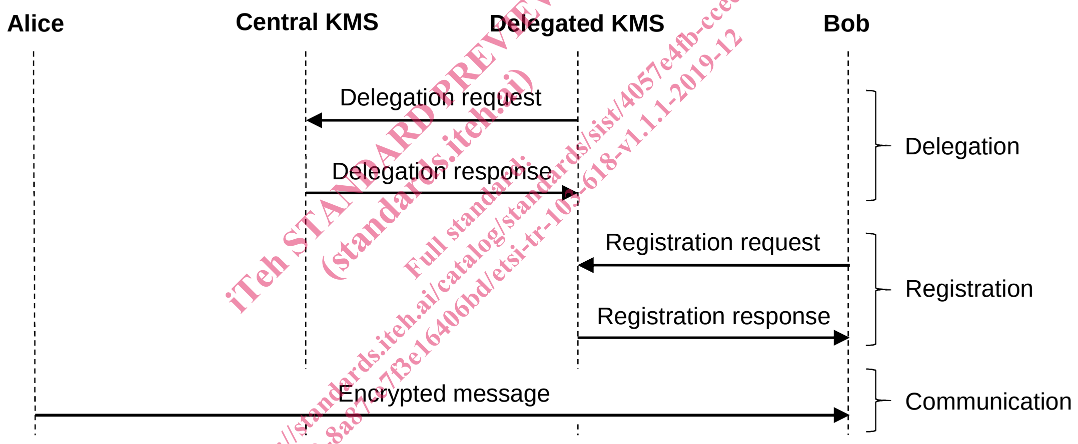

Figure 3: Encrypted communication with HIBE

In practice, traditional public-key cryptography is often used in an authenticated key exchange to establish a shared symmetric key between two or more users. Identity-based cryptography can be used to provide similar functionality. In this case, Alice generates a symmetric key and sends it to Bob encrypted under his public identifier. If Bob can successfully decrypt the symmetric key, then this implicitly authenticates Bob to Alice. For mutual authentication, Alice can use an identity-based signature to digitally sign the message with a key that is bound to her public identifier. Alternatively, Bob can send Alice a response message that is encrypted under her public identifier (Figure 4).

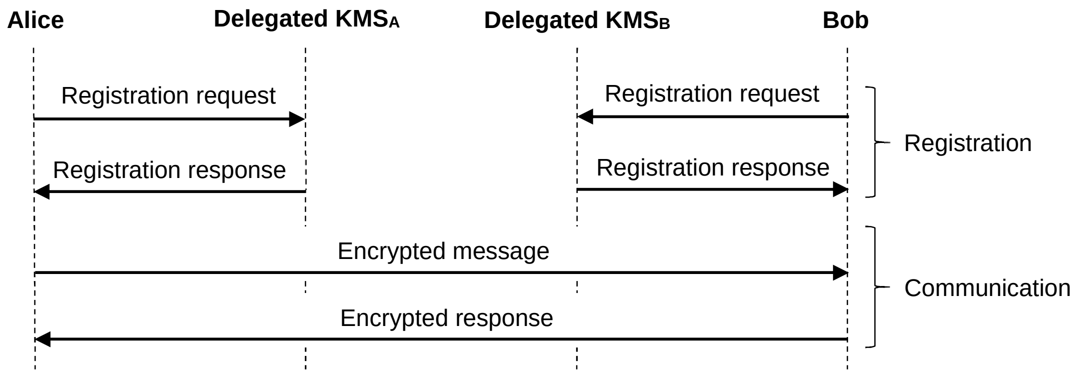

Figure 4: Mutual authentication with HIBE

4.3 Discussion

A fundamental feature of most IBE and attribute-based encryption (ABE) schemes is the reliance on a trusted KMS to derive user private keys based on their public identifiers or attributes. In a traditional PKI, if an adversary can gain access to the CA or compromise its private key, then they are potentially able to impersonate any user in the system and read encrypted communications via man-in-the-middle attacks. However, if an adversary can gain access to the KMS or compromise its private key, then they are potentially able to read any encrypted communications on the system including messages that were sent before the comprise. There are several responses and mitigations to this:

- To be able to read a user's communications an attacker would need both to obtain the private key and be able to intercept or otherwise access the encrypted messages. In many real-wold deployments, the KMS is based in a secure location and user key derivation is performed off-line. Network access is only required during the user provisioning process itself which is typically only performed at initial registration and then potentially at monthly or yearly intervals after that.

- The use of HIBE can further limit the exposure of the central KMS as network access is only required during the provisioning of a small number of sub-KMSs which is likely to be infrequent. Similarly, the compromise of a sub-KMS only affects the users managed by that KMS and KMSs below it in the hierarchy rather than all users in the system.

- There are cryptographic mechanisms that allow split or multi-party derivation of the user private keys with a distributed KMS [i.4] that requires the co-operation of more than one authority. The shares of the user private key can then be stored at different secure locations. An adversary would need to gain access to multiple authorities or comprise private data in multiple places in order to recover the full private key for a user.

- For some deployments, there are valid requirements for the organization to be able to access user private keys. For example, there might be regulatory requirements to audit encrypted communications on the enterprise network. Similarly, it allows the recovery of encrypted corporate data in the event that a user loses their private key. In examples such as these, it is important that policies are put in place to ensure that access is restricted to properly authorized individuals for valid regulatory or organizational reasons, and that they are only allowed access to a limited set of well-specified private keys.

The other area where IBE schemes differ significantly from a traditional PKI is revocation of compromised user private keys. In a PKI, the revocation is typically handled using Certificate Revocation Lists (CRLs) periodically issued by the CA, or checks performed via the Online Certificate Status Protocol (OCSP). However, revocation is more complicated for IBE schemes as a user's private key is intrinsically linked to their identifier. There are a few different approaches that can be taken:

- The simplest option is to include a time and date as part of the public key in order to limit the validity period for the compromised private key [i.4]. The equivalent of a CRL could then be used to prevent further messages being encrypted to the compromised user for the remainder of the validity period. Messages encrypted before the compromise would still potentially be vulnerable. Further, all users in the system would need to securely contact the KMS to obtain their new private keys for next validity period.