ETSI Security Week 2020 goes virtual!

Even More Advanced Cryptography
ETSI Standardization in Advanced Cryptography

Presented by: François Ambrosini, Umlaut
Christoph Striecks, AIT Austrian Institute of Technology
<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monday 8 June</td>
<td>3pm CET</td>
<td>5G Deployment</td>
</tr>
<tr>
<td>Tuesday 9 June</td>
<td>10.30am</td>
<td>SSP: The New Smart Secure Platform - A High Level Introduction</td>
</tr>
<tr>
<td></td>
<td>4.45pm</td>
<td>SSP: The New Smart Secure Platform - The Technical Realisation</td>
</tr>
<tr>
<td>Wednesday 10</td>
<td>10.30am</td>
<td>Insight into the First Steps of the Cybersecurity Act Reality</td>
</tr>
<tr>
<td>June</td>
<td>11.30am</td>
<td>Consumer IoT Security Standards</td>
</tr>
<tr>
<td>Thursday 11</td>
<td>10.00am</td>
<td>Consumer IoT Security Standards</td>
</tr>
<tr>
<td></td>
<td>11.30am</td>
<td>Consumer IoT Security – Certification Schemes</td>
</tr>
<tr>
<td></td>
<td>3pm</td>
<td>ETSI Standardization in Advanced Cryptography</td>
</tr>
<tr>
<td>Monday 15 June</td>
<td></td>
<td>3pm SKINNY LATTE: Scalable Hierarchical Identity Based Encryption over Lattices</td>
</tr>
<tr>
<td>Tuesday 16 June</td>
<td>10.30am</td>
<td>5G Security Evolution</td>
</tr>
<tr>
<td>Wednesday 17</td>
<td>10.00am</td>
<td>5G Network Certification</td>
</tr>
<tr>
<td>June</td>
<td>10.00am</td>
<td>Security Challenges and Regulatory Aspects</td>
</tr>
<tr>
<td>Thursday 18</td>
<td>3pm</td>
<td>Fully Homomorphic Encryption</td>
</tr>
<tr>
<td>Friday 19 June</td>
<td>10.30am</td>
<td>Industry Applications and Use Cases for Advanced Cryptography</td>
</tr>
</tbody>
</table>
ETSI Standardization in Advanced Cryptography
Moderated by François Ambrosini, Umlaut

- Attribute-Based Encryption for Strong Access Control: TS 103 532
  Christoph Striecks, AIT Austrian Institute of Technology

- Identity-Based Cryptography: ETSI Technical Report
  François Ambrosini, Umlaut

- Quantum-Safe Identity-Based Encryption: TR 103 618
  Christoph Striecks, AIT Austrian Institute of Technology
Attribute Based Encryption for Strong Access Control: TS 103 532
Agenda

✔ Introducing Attribute-Based Encryption (ABE) and context*
✔ Motivating ABE for strong access control
✔ TS 103 532: Attribute-Based Encryption Toolbox
✔ Future directions

*With slides from François Ambrosini.
Introducing ABE – Attribute Based Encryption

Attribute Based Encryption standardized in two technical specifications

✔ TS 103 458, “Application of Attribute Based Encryption (ABE) for PII and personal data protection on IoT devices, WLAN, cloud and mobile services - High level requirements”

✔ TS 103 532, “Attribute Based Encryption for Attribute Based Access Control”

First standardization effort worldwide, 2016, done in TC CYBER

First introduced by Sahai and Waters in 2004, “Fuzzy Identity Based Encryption”
Attribute Based Encryption: Properties & Benefits

Encrypt and manage access control rights, within one cryptosystem

✔ ABE combines encryption and access control

Very flexible access control

✔ No need to grant rights at the moment of encryption

✔ Grant new rights at any time, infinity of policies under some ABE schemes

Access control enforced at mathematical level – high security assurance
Data Encryption + Sharing: Industrial IoT case example

Data lake

Value chain actors share the cryptosystem

Data streams

Factory

Factory equipment

Headquarters

Third-parties (insurance, service providers...)

Downstream & upstream (value chain)
Motivating ABE for Strong Access Control
Attribute Based Access Control

Project Overview

The current rapid growth of electronic commerce, the proliferation of computer networks, and the advancement of technology have led to an increased number of logical access control methods. In November 2007, the NIST Information Technology Laboratory (ITL) initiated the Attribute Based Access Control (ABAC) project. The ABAC project was intended to develop a comprehensive framework that can be used to manage access within and between organizations across the Federal enterprise. In December 2011, the FICAM Roadmap and Implementation Plan v2.0 took the next step of calling out ABAC as a recommended access control model for promoting information sharing between diverse and disparate organizations.

NIST Special Publication 800-162 (Jan 2014)
Attribute-Based Access Control (ABAC, simplified)

Role: Engineer
Area: Development
Time: 2020

PEP & PDP (Policy Enforcement Point & Policy Decision Point)

Policy Folder A:
- Scientist
  AND Research

Policy Folder B:
- Engineer
  AND Development
  AND 2020

Policy Folder C:
- Engineer
  OR 2020
Attribute-Based Access Control (ABAC, simplified)

Role: Scientist
Area: Research
Time: 2020

PEP & PDP
(Policy Enforcement Point & Policy Decision Point)

Policy Folder A: Scientist AND Research

Policy Folder B: Engineer AND Development AND 2020

Policy Folder C: Engineer OR 2020
Attribute-Based Access Control (ABAC)

Advantage: fine-grained access to data, defined on attributes and policies with strong PEP/PDP mechanisms

Disadvantage: massive trust in software-based PEP/PDP implementations (software implementation often prone to errors)

Can we do better?

Yes! Enforcing access control through cryptography using Attribute-Based Encryption
Crypto 1.0: Secret-Key Encryption

Security guarantee: looks random without knowing $k$

Properties:
- Enables secure one-to-one communication
- Key $k$ has to be distributed before (how?)
- Keys have to be maintained for each partner (i.e., huge overhead)
- Encryption is all-or-nothing (keys have one-to-one relationship)
Crypto 2.0: Public-Key Encryption

Properties:
- Enables secure one-to-one communication
- Solves key-distribution problem (pk is publicly available)
- Key pk has to be authenticated (e.g., by using heavy PKI)
- Encryption is all-or-nothing

Security guarantee: looks random without knowing sk
Crypto 4.0: Attribute-Based Encryption

Security guarantee: looks random without knowing secret keys

Properties:
- Enables fine-grained one-to-many communication
- Enforces access control on the cryptographic level
- Many secret keys for one set of pp (hence, less-heavy PKI needed)
- Need of pp-related authority KMS that distributes secret keys KMS
Work on ABE schemes within ETSI TC CYBER

Central idea

✓ Find ABE schemes for ABAC suitable for IoT, cloud, and mobile

Main goals

✓ Provide cryptographic ABE toolbox specification,
✓ with strong security guarantees,
✓ for key exchange and message encryption,
✓ and modularity feature for future schemes.
Concrete schemes, specified in TS, can be modularly exchanged (e.g., with future schemes)

Attribute-based key exchange and encryption schemes with mild security guarantees

Attribute-based key exchange and encryption schemes with strong security guarantees; recommended
ABE Toolbox Takeaway

Developer may choose from TS 103 532 between

- 4 specified attribute-based schemes
- with 2 functionalities (key exchange or message encryption)
- and 2 levels of security (mild or strong)

Modularity feature

- Also recently developed schemes (which are, e.g., quantum-safe) that fit the requirements listed in TS 103 532 supported
- Please consider contributing such new schemes in ETSI TC CYBER
Further Work on ABE

Work continues in TC CYBER

✓ Conformance & interoperability testing for ABE planned

Continuously ongoing work in academia

✓ News: improved FAME scheme published only last week (PKC 2020)
✓ Practical quantum-safe ABE identified as key topic

ABE in in EU research projects

✓ ASCLEPIOS (asclepios-project.eu), ABE for Health
✓ SAFEcrypto (safecrypto.eu), quantum-safe ABE
✓ FENTEC (fentec.eu), implementations for FAME and GPSW schemes
Future directions

Promising new field: Functional Encryption (FE)

✓ FE is a generalisation of ABE (and also of IBE) and even more powerful (e.g., allows for privacy-preserving computation)


✓ Most flexible scheme by Chotard et al. “Decentralized Multi-Client Functional Encryption for Inner Product”, 2018

✓ EU project FENTEC (fentec.eu) implements FE technology already

Thank you!
Agenda

✔ Introducing Attribute-Based Encryption and ETSI TR 103 719
✔ IBE in more details, operations and use cases
✔ Measures for secure and successful deployments
✔ Conclusion and next steps
What is Identity Based Encryption?

✔ Asymmetric (public key) cryptography

✔ The public key is a string of the receiver (and sender) choosing
  ✔ Straightforwardly tied to an identity
  ✔ The cryptographic scheme works around this invariant

Properties of IBE & IBC

✔ User friendly

✔ Can be extended with access control

✔ Well suited for operations in controlled environment
  ✔ Auditability
  ✔ Relies on trusted third party
ETSI TR 103 719 – Guide to Identity Based Cryptography

✓ Demystify Identity Based Cryptography
  ✓ Identity Based Encryption
  ✓ Identity Based Signature

✓ Guidance for developer to adopt IBC
✓ Identify key issues of IBC deployment
✓ Identify standardisation gaps
✓ Relation to Attribute Based Encryption
Identity Based Encryption by example

Sender

Recipient

user1@example.org
Identity Based Encryption – cryptosystem operations

Key Management System

- **Setup**
  - $\text{MSK, MPK}$

- **Extract**
  - $\text{SK}_{ID}$

- **Encrypt**
  - $\text{MPK, ID, M}$

- **Decrypt**
  - $\text{MPK, SK}_{ID}, C_{ID}$
Identity Based Encryption – use cases

Pure identity

✔ E-mail

✔ One-on-one and group communications

✔ Critical communications

Identity extended for access control

✔ Set by the sender and enforced by the KMS

✔ MAC, RBAC, encrypt into the future, encrypt to future users

✔ Locally irreversible encryption

✔ Automated systems (machine to machine, IoT)

ID: “identity”

ID: “group = group-identity”

ID: “identity | (role = accounting OR role = auditor) AND date > ...”
Identity Based Encryption – risk analysis

Common threats applied to IBC

✔️ Key Management System

✔️ Communications between IBC clients and the Key Management System

✔️ Communications between IBC clients

✔️ Key protection

Threats specific to IBC

✔️ Attacks through the identity string

✔️ Information security, privacy and data protection for the identity string
Identity Based Encryption – deployment challenges

✔ Simplicity for the user means the complexity is taken over by the infrastructure

✔ Resolution protocols
  ✔ From a target identity, how does the sender configure the crypto?
  ✔ Limit reliance on the Key Management System

✔ Bootstrapping trust

✔ PKI management for IBC
  ✔ Secret sharing schemes and delegation schemes for the Master Secret Key

✔ Use of IBC in fully open systems
Conclusions

- IBC is a promising field of cryptography with numerous applications
- ETSI TR 103 719 spearheads the standardisation work
- Example HIBE scheme in the next presentation

Thank you!
Quantum-Safe (Hierarchical) Identity-Based Encryption: TR 103 618

Presented by: Christoph Striecks
For: ETSI Security Week 2020

AIT Austrian Institute of Technology
11.06.2020

© ETSI
Agenda

✔ Motivating quantum-safe cryptography
✔ Introducing (Hierarchical) Identity-Based Encryption (HIBE)
✔ ETSI TR 103 618: “Quantum-Safe Identity-Based Encryption”
✔ Future directions
What is Quantum-Safe Cryptography?

Not quantum cryptography

✓ i.e., not quantum key distribution, often also called post-quantum cryptography

Rather

✓ Cryptographic systems that run on classical computers and are considered to be resistant to quantum attacks

✓ For example: (public-key) encryption schemes, signature schemes, key-distribution, and also HIBEs
The ETSI Security Week 2020 goes virtual!

Many presentations that were to be given during the ETSI Security Week will be given virtually from 8 until 19 June.

Thanks to the willingness and additional efforts of nearly 50 Programme Committee Members and Speakers, we are able to offer 14 different webinars corresponding more or less to what the ETSI Security Week should have been this year!

The ETSI Security Week 2020 is organized around four technical threads:
In an Advent of Powerful Quantum Attackers

Shors’s algorithm (1994):
- Factoring and discrete logarithms efficient

Grover’s algorithm (1996): square-root speedup
- double key size (symmetric encryption)
- double output size (hash functions)
- $N$ bit $\rightarrow 2N$ bit
When are Quantum Computers Powerful Enough?

Problem

✔ Quantum computers break currently deployed public-key cryptography

✔ Situation of **powerful quantum computers** unclear at the moment, but research is advancing fast

✔ However, what we know: it takes time to change deployed cryptography

Solution

✔ To have well studied cryptographic schemes and standards available when required

✔ **Hence**: standardization work ongoing, e.g., for quantum-safe key-exchange, digital signatures, and other primitives (ETSI, NIST, ANSI, IEEE, IETF & IRTF, ISO, BSI, ...
Introducing (Hierarchical) Identity-Based Encryption
Introducing (Hierarchical) Identity-Based Encryption

Quantum-safe identity-based encryption in ETSI technical report
✓ TR 103 618 v1.1.1, “Quantum-Safe Identity-Based Encryption”, 12-2019

Cryptographic background
✓ Idea of IBE dates back to 1984 by Shamir, first constructions only in 2000 and 2001
✓ First constructions by Gentry, Silverberg in 2001 “Hierarchical ID-Based Cryptography”
✓ First quantum-safe HIBE constructions:
  • Agrawal, Boneh, Boyen, 2010 “Efficient lattice (H)IBE in the standard model”
  • Cash, Hofheinz, Kiltz, Peikert, 2010 “Bonsai trees, or how to delegate a lattice basis”
Quantum-Safe HIBE: Properties & Benefits

In general

✔ Any hierarchy of strings, e.g., “Enterprise A | Smith@etp.com”, can serve as public key in HIBEs
  • More fine-grained approach compared to common public-key cryptography
  • Hierarchies can be built to use delegation of decryption rights (e.g., within companies)

✔ But most distinguishing feature here is quantum-safeness: conjectured resistance against quantum-scale attacker

✔ Problem: Shor’s algorithms is a danger to common public-key cryptography also to conventional HIBE schemes that are not quantum-safe
Crypto 1.0: Secret-Key Encryption

Security guarantee: looks random without knowing $k$

Properties:
- Enables secure one-to-one communication
- Key $k$ has to be distributed before (how?)
- Keys have to be securely maintained for each communication partner (i.e., huge overhead)
- Encryption is all-or-nothing (keys have one-to-one relationship)
Crypto 2.0: Public-Key Encryption

Security guarantee: looks random without knowing $sk$

Properties:
- Enables secure one-to-one communication
- Solves key-distribution problem (pk is publicly available) compared to secret-key encryption
- Key pk has to be authenticated (e.g., by using heavy PKI)
- Encryption is all-or-nothing
Crypto 3.0: Identity-Based Encryption

Security guarantee: looks random without knowing secret keys

Properties:
- Enables one-to-many communication
- Only public string, e.g., email address, needed
- Many sk keys for one set of pp ("less-heavy" PKI needed)
- Need of pp-related authority KMS that distributes keys
Crypto 3.5: Hierarchical Identity-Based Encryption

Security guarantee: looks random without knowing secret keys

Properties:
- Enables one-to-many communication
- Only public hierarchical identifier needed
- Many Sub-KMSs possible for one set of pp
- Sub-KMSs can delegate secret keys
- Need of authorities (Sub-)KMS that distribute keys
Work on HIBE schemes within ETSI TC CYBER QSC

Central idea:

✔ Proposal for a quantum-safe HIBE in ETSI TR 103 618

Main goals:

✔ What functionality will be provided by (H)IBEs?

✔ Example use cases

✔ High-level description of a quantum-safe HIBE solution on structured lattices (mathematical problem that is conjectured to be quantum-safe)
Work on HIBE schemes within ETSI TC CYBER QSC

Example use-cases for enterprise and IoT applications

✓ In General: suitable for governments and enterprises to ease key management
✓ HIBE: mirrors large organizations that can have a central KMS with several sub-KMSs
✓ IBE: public safety and mission critical applications which require secure one-to-one, group, and broadcast communications (benefit is low-latency key management)

Presented scheme

✓ LATTE (from structured lattices) with performance evaluation (fast encryption and decryption) on strong and embedded processors
Future directions

Ongoing work in academia
- Research on optimizations & more secure schemes for HIBEs
- Efficient revocation is an important topic
- Also more efficient quantum-safe HIBEs are researched
  - See ETSI Security Week 2020 talk on “Skinny LATTE” by Sarah Mac Carthy, 15 June 2020, 15.00-16.00 CEST

Functional Encryption (FE) as future topic
- Generalizes IBE and even allows computation on encrypted data
- Quantum-safe FE for inner products already available

Thank you!
Questions & Answers
Upcoming webinars in the thread
Even More Advanced Cryptography:

15 June, 3.00pm: SKINNY LATTE: Scalable Hierarchical Identity Based Encryption over Lattices,

18 June, 3.00pm: Fully Homomorphic Encryption

19 June, 10.30am: Industry Applications and Use Cases for Advanced Cryptography
Thank you for joining this webinar!

Find the full ‘ETSI Security Week 2020 goes virtual’ programme at

www.etsi.org/etsisecurityweek