Security Conference 2022

Identity in cryptography: A review of IBC/ABC and IBE/ABE (from TR 103 719)

Scott Cadzow, C3L UK

A summary of TR 103 719

- The purpose of TR 103 719 was to describe the use and application of Identity-Based Cryptography (IBC) applied to encryption, (IBE), and to digital signature (IBS).
- The target was to allow non-experts in the technology of IBC to be able to gain an understanding of the technology, its domains of application, and its required environment

What is different in IBC from other PKCs?

It is not fully public

- It is managed within a closed environment
- User secret keys are derived by a trusted central authority, the Key Management Service (KMS), rather than users

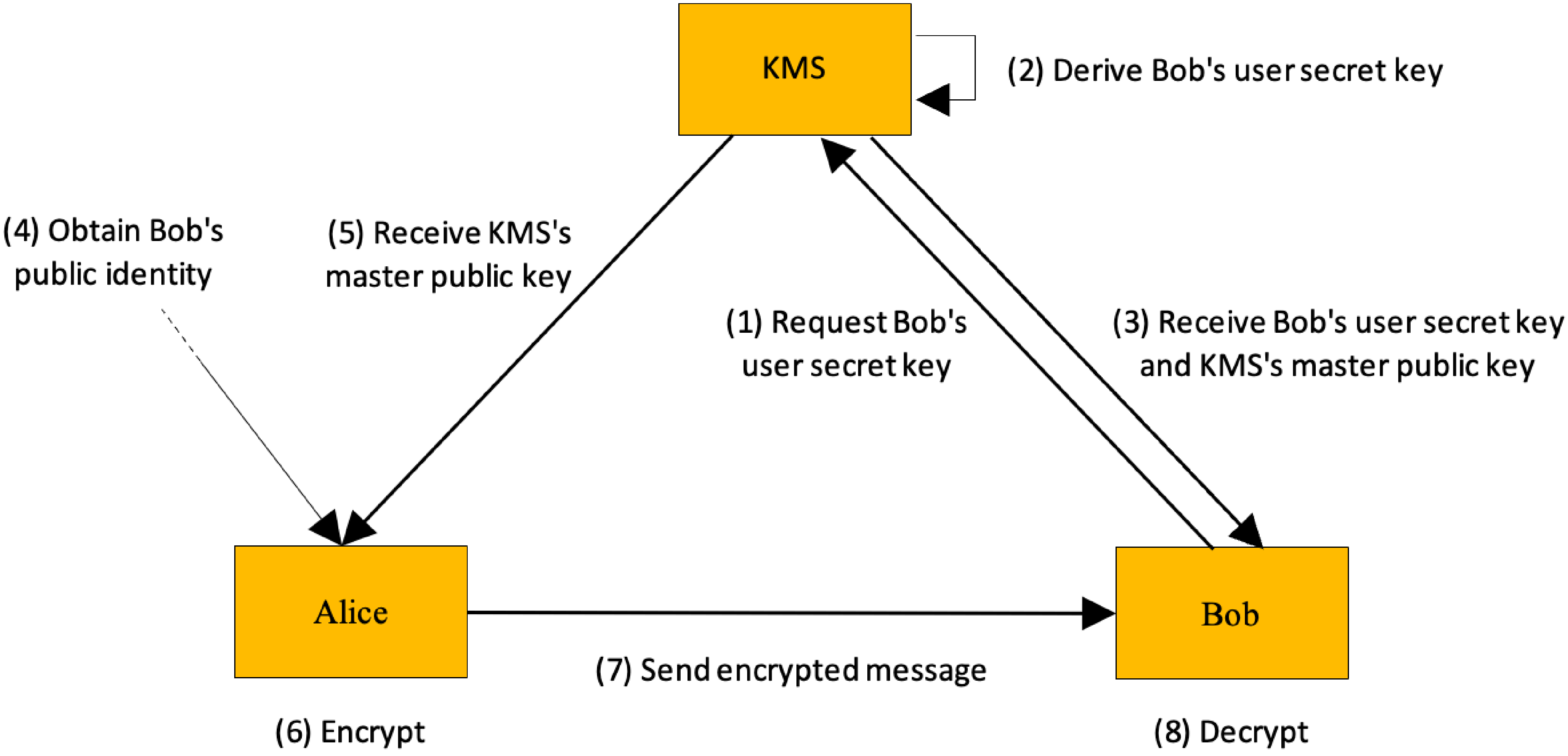
It combines semantics with the identity

- For example email addresses have semantic value

It supports low resource devices

- Supported in a proxy mode

Identity-Based Encryption (IBE)



KMS

(2) Derive Bob's user secret key

(4) Obtain Bob's public identity

(5) Receive KMS's master public key

(1) Request Bob's user secret key

(3) Receive Bob's user secret key and KMS's master public key

Alice

Bob

(7) Send encrypted message

(6) Encrypt

(8) Decrypt

Differences - IBC vs PKC Key infrastructure

Security Conference 2022

- Conventional PKC solutions require a means of binding a public key to the identity, or some other attribute, of its user.
  - A common method for doing this is via public key certificates that are managed in a Public Key Infrastructure (PKI).
  - Certificates are issued by a trusted Certificate Authority (CA) who needs to ensure that the user requesting the certificate is the legitimate owner of the public key
- In an IBC scheme, the public identities can contain explicit semantic content, such as the e-mail address of the user, and be integrated with the protected service.
  - Secret keys are derived by a trusted KMS who needs to ensure that the user requesting the secret key is the legitimate owner of the identity

Differences - IBC vs PKC Key generation

Security Conference 2022

- The master key pair for a PKI (root key) is generated by the CA. The root public key needs to be distributed to all users of the service so that they can verify user certificates.
  - Conventionally user key pairs are generated by users
- The master key pair for an IBC scheme is generated by the KMS
  - The master public key needs to be distributed to all users of the service so that they can use it in encryption, for an IBE scheme, or in verification, for an IBS scheme.
  - User secret keys can only be derived by the KMS and need to be sent securely to the user

Differences – IBC vs PKC Key storage

- The root key for a PKI needs to be stored securely by the CA
  - Users need to store their user secret keys securely.
  - Certificates containing the user public encryption keys need to be retrievable from a central repository.
  - Certificates containing user public verification keys can be sent along with the signed message.
- The master secret key for an IBC scheme needs to be stored securely by the KMS.
  - User secret keys can be rederived by the KMS so do not need to be retained by the user in order to provide resilience and recovery.
  - If a user does retain their secret keys they need to store them securely.
  - User public identities can be integrated with the protected service and so do not need to be retrievable from a central repository

Differences - IBC vs PKC Key lifetimes

- The master key pair in a PKI tends to be long lived and updated infrequently.
  - Certificates containing user public keys tend to be much shorter lived and updated regularly.
  - Certificates include explicit expiry dates for user public keys, so a new certificate needs to be issued when the old certificate expires.
- The master key pair in an IBC scheme tends to be long lived and updated infrequently.
  - Public identities such as e-mail addresses do not expire, but the identity can be extended to include an expiry date.
  - If the identity does include an expiry date, then a secret key needs to be derived for the new identity when the old identity expires

Differences - IBC vs PKC Key compromise

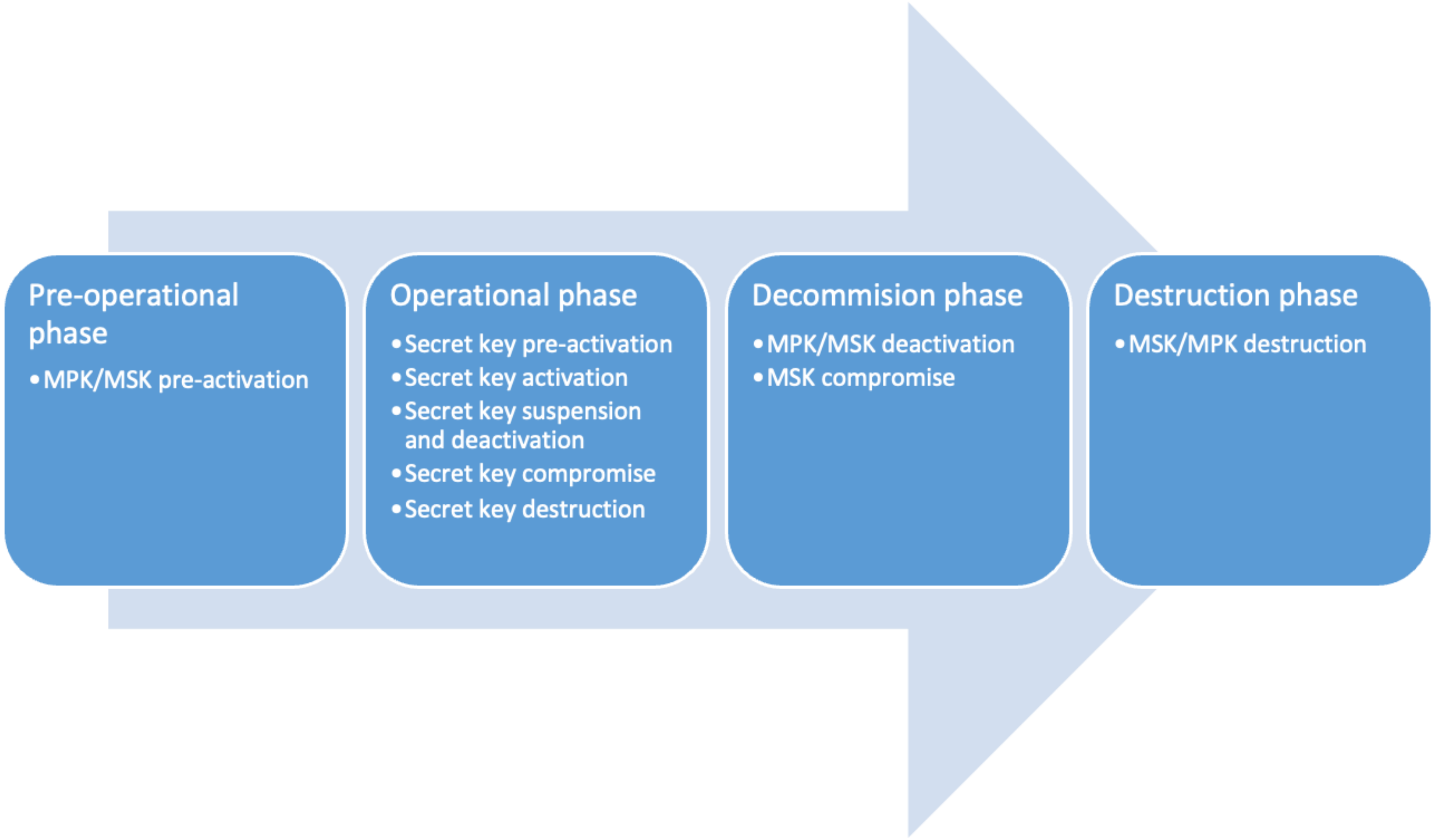
- If the master secret key for a PKI is compromised, then an attacker can forge a certificate for any user of the service.
  - If the certificate contains a user public encryption key, then the attacker can impersonate the user and read any messages intended for the real user that are encrypted using the forged certificate. However, the attacker would not be able to read any messages sent to the real user before the compromise.
  - If the certificate contains a user public verification key, then the attacker can impersonate the user and sign messages that would verify correctly with the forged certificate. However, the signed messages would not verify correctly with a genuine certificate previously issued to the user.
- If the master secret key for an IBC scheme is compromised, then an attacker can derive the user secret key for any user of the service.
  - For an IBE scheme, the attacker would be able to read any message sent to the user including messages that were sent before the compromise.
  - For an IBS scheme, the attacker would be able to impersonate the user and forge signatures that are indistinguishable from a genuine signature for that user.

Differences - IBC vs PKC Key revocation

Security Conference 2022

- In a PKI, user certificates can be revoked by the CA and replaced by new certificates issued with fresh user key pairs.
  - Short-lived user certificates can make revocation simpler as new certificates will already be needed when the old certificates automatically expire.
  - Revoking the master key pair is more difficult and would require all user certificates to be reissued.
- In an IBC scheme, user public identities such as e-mail addresses are static and so cannot be revoked or reissued easily.
  - If the public identity is extended to include an expiry date, then revocation is automatic at the end of the lifetime of the identity and a fresh user secret key can be derived for the new identity.
  - Revoking the master key pair is more difficult and would require all user secret keys to be rederived

The IBC key lifecycle



Pre-operational phase

- MPK/MSK pre-activation

Operational phase

- Secret key pre-activation
- Secret key activation
- Secret key suspension and deactivation
- Secret key compromise
- Secret key destruction

Decommision phase

- MPK/MSK deactivation
- MSK compromise

Destruction phase

- MSK/MPK destruction

IBC use cases

- Where it fits:
  - Government and enterprise
  - Public safety and mission critical
  - Internet of Things (IoT)
  - Intelligent transport systems (ITS)
- Functions it offers:
  - Access control
  - Unicast/multicast/group/broadcast encryption
  - Encrypt into the future
  - Delegation of duty
  - Locally irreversible encryption

Where it fits

- Government and enterprise
    - The primary advantage of IBC is that conventional centralized information and processing models used in corporate e-mail and file sharing schemes can be straightforwardly mapped to IBC
- Public safety and mission critical
    - Public safety and mission critical applications which require secure one-to-one, group and broadcast communications are ideally suited as IBE candidates. Low-latency key management is important in order that a secure communication channel is available as soon as possible during an incident, and where there is a need to support direct communications between users if or when network infrastructure is unavailable
- Internet of Things (IoT)
    - The primary advantage here is that the key management is lightweight and communications between devices do not need to involve the central infrastructure. In addition, the algorithmic complexity of IBC is not overly high for the encrypt/decrypt functions to be performed on a relatively constrained device
- Intelligent transport systems (ITS)
    - For further study but the registration number (UK) or the VIN could be used as a public identity to address individual vehicles

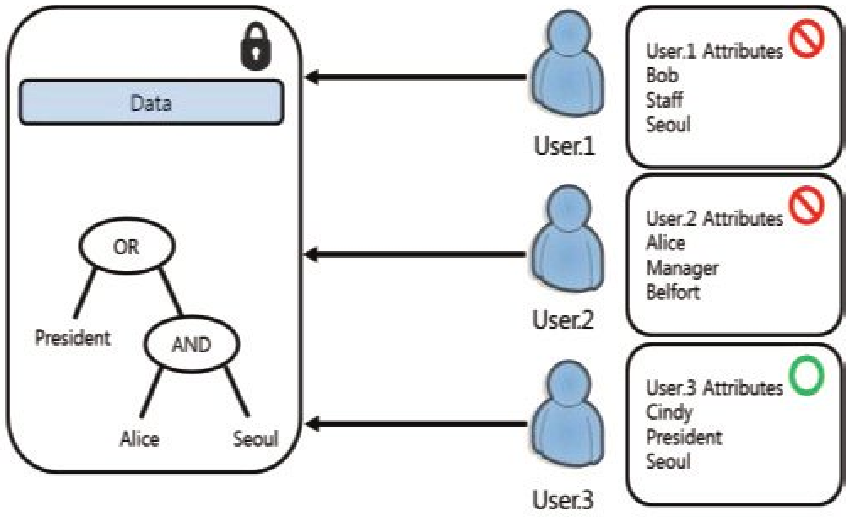
Functions it offers

- Access control
  - Part of attribute based access control
- Unicast/multicast/group/broadcast encryption
  - Tailoring the identity to 1, many or all
- Encrypt into the future
  - If the user isn't yet active but anticipated a message can be sent to them as long as they are configured in the system (say an employee due to start on Monday but known about the week before)
- Delegation of duty
  - Essentially this allows e-mail forwarding to work even with IBE email
- Locally irreversible encryption
  - Allows lightweight devices to use proxies and limit access

Identity based vs attribute based

- Identity is an attribute
  - IBE assumes semantic attribution of the identity (e.g. email address) whereas ABE has more nuance in its semantic attribution (i.e. no direct semantic information in the attribute set)
- Two forms of ABE for access control:
  - Ciphertext policy → associates secret keys with attributes from an attribute universe and ciphertexts with access policies
    - To generate the secret key the ABE authority takes as input the master secret key $MSK_{CP\text{-}ABE}$, and an attribute set A, and outputs a secret key SK_A.
  - Key policy → associates ciphertexts with attributes from an attribute universe and secret keys with access policies
    - To generate the secret key the ABE authority takes as input the master secret key $MSK_{KP\text{-}ABE}$, and an access policy AP, and outputs a secret key SK_{AP}.
- ABE access control determines by attributes who has access to encrypted data

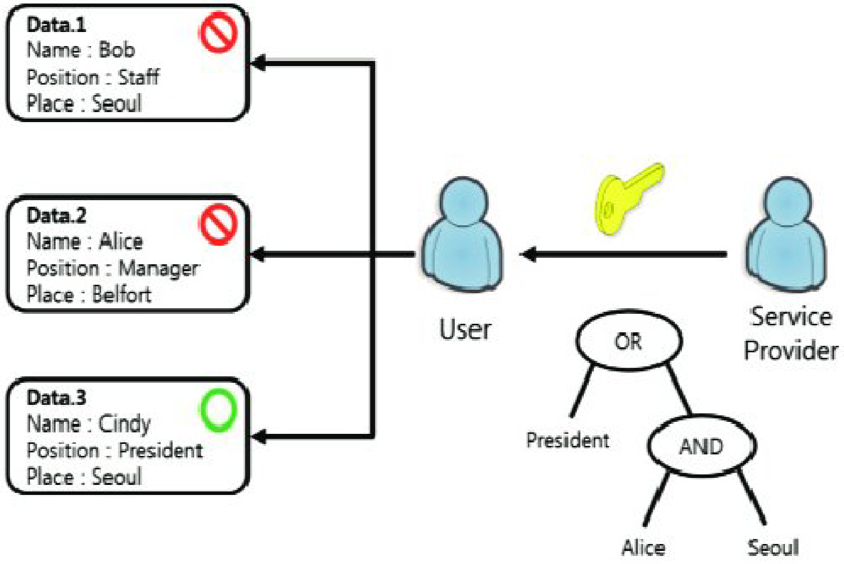
Difference between key policy and ciphertext policy ABE?



User.1 Attributes
Bob
Staff
Seoul

User.2 Attributes
Alice
Manager
Belfort

User.3 Attributes
Cindy
President
Seoul



Data.1
Name : Bob
Position : Staff
Place : Seoul

Data.2
Name : Alice
Position : Manager
Place : Belfort

Data.3
Name : Cindy
Position : President
Place : Seoul

Policy:
If {(position=PRESIDENT) OR ((name=ALICE) AND (place=SEOUL))} ➔ Grant access, else deny access

In both instances Cindy gets access, in one case unlocking the key, in the other by mapping to the policy

In summary

- ABC and IBC each make the key “a real thing”
- Who you are (identity) or what you are (attributes)
- The key may have semantic context built in (identity in the form of an email address to access encrypted email say)
- Knowledge of the public key and its nature gives no clue to its use as a key
    - An email address is still an email address
    - An attribute (say a role) is still that attribute

Thank you for your attention

Follow us on:

Any (further) questions?

scott@cadzow.consulting