

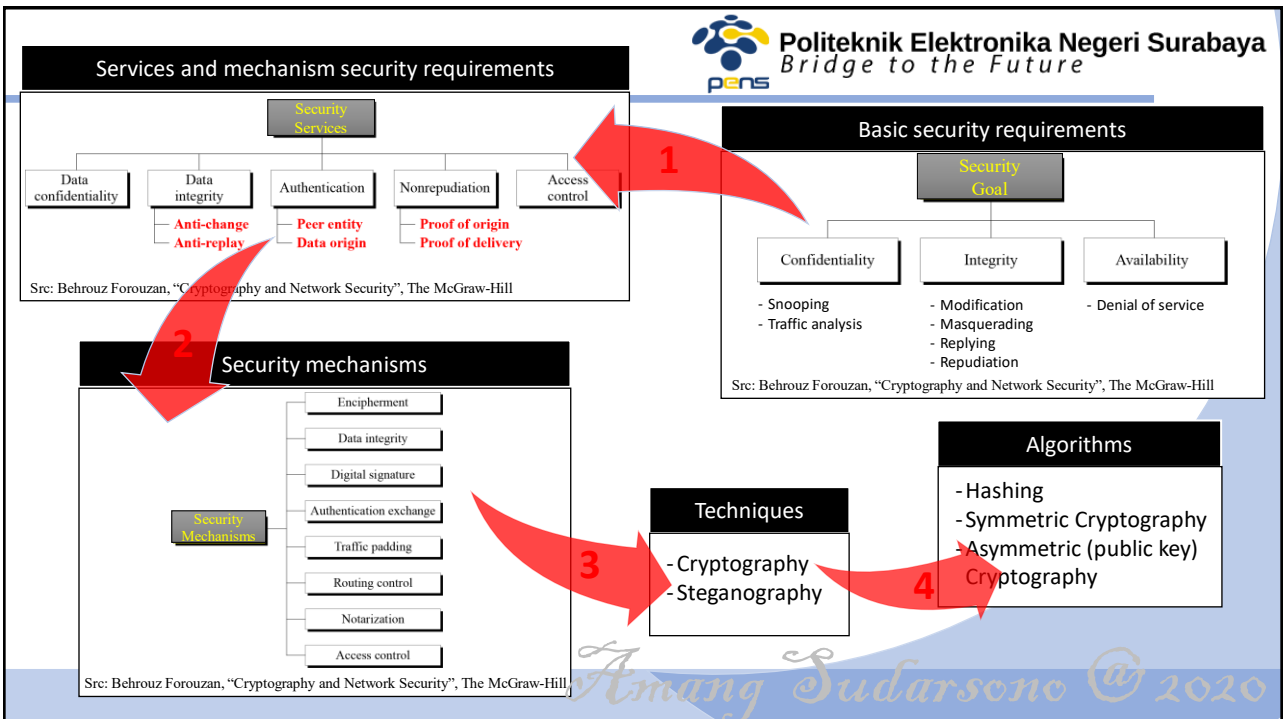
Research Topics on Anonymous Authentication

Agenda:

- *Overview & Background*
- *Some Implementations*

Amang Sudarsono
 Thursday, August 27, 2020
<http://amang.lecturer.pens.ac.id>

1



2

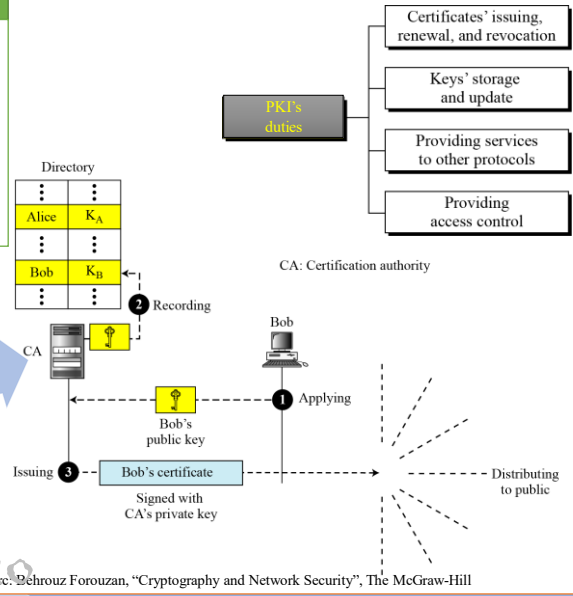
Key Distribution

Symmetric Crypto

- Each pair of communicating entities needs a shared key
 - If n -party system, it needs $n(n-1)/2$ distinct keys in the system and each party needs to maintain $n-1$ distinct keys
- OR it is only n distinct keys if involving a KDC, etc

Asymmetric Crypto

- Public Announcement
- Trusted Center
- Controlled Trusted Center
- Certification Authority, X.509, and Public-Key Infrastructures (PKI)



Amang Sudarsono @ 2020

3

Entity Authentication

a technique lets one party prove the identity of another party. It can be a person, a process, a client, or a server. It's identity needs to be proved (**claimant**); the party that tries to prove the identity of the claimant is called the **verifier**

Message authentication vs Entity Authentication

- might not happen in real time vs real time,
- simply authenticates one message & need to be repeated for each new message vs authenticate the claimant for entire duration of a session.

Anonymous Authentication

Zero-knowledge

The claimant proves to the verifier that she knows a secret, without revealing it. The interactions are designed to not revealing or guessing the secret

Password-based

- either Fix or One-time

Challenge-response

- either using symmetric-key, keyed-hash func., asymmetric-key or digital signature


The claimant proves that she knows a secret **without sending it**
The claimant reveals her secret

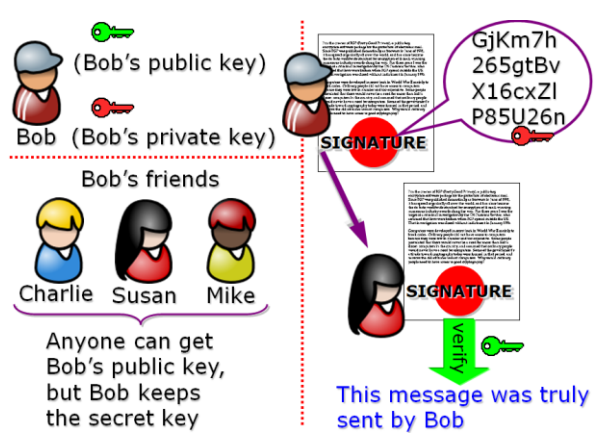
Amang Sudarsono @ 2020

src: Behrouz Forouzan, "Cryptography and Network Security", The McGraw-Hill

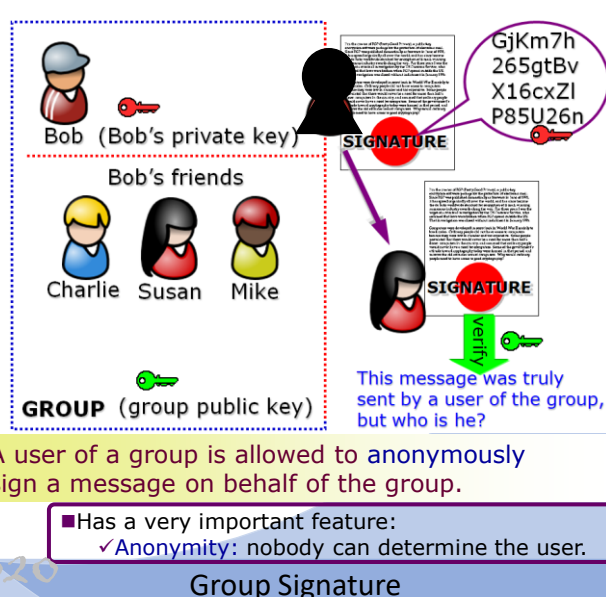
4

Conv. Signature vs Group Signature





Digital Signature




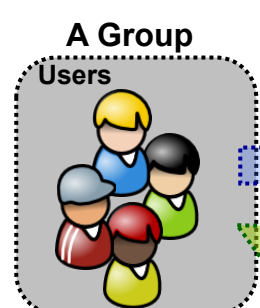
Group Signature

Amang Sudarsono @ 2020

5

Group Signature Mechanism






A Group Users

Made by a user. But, I do not know who he is.

ANONYMOUS

Signature




Verifier
■ Verifies sig.

■ Only issued by the GM

■ Contains the keys issued by a legal authority

Certificate

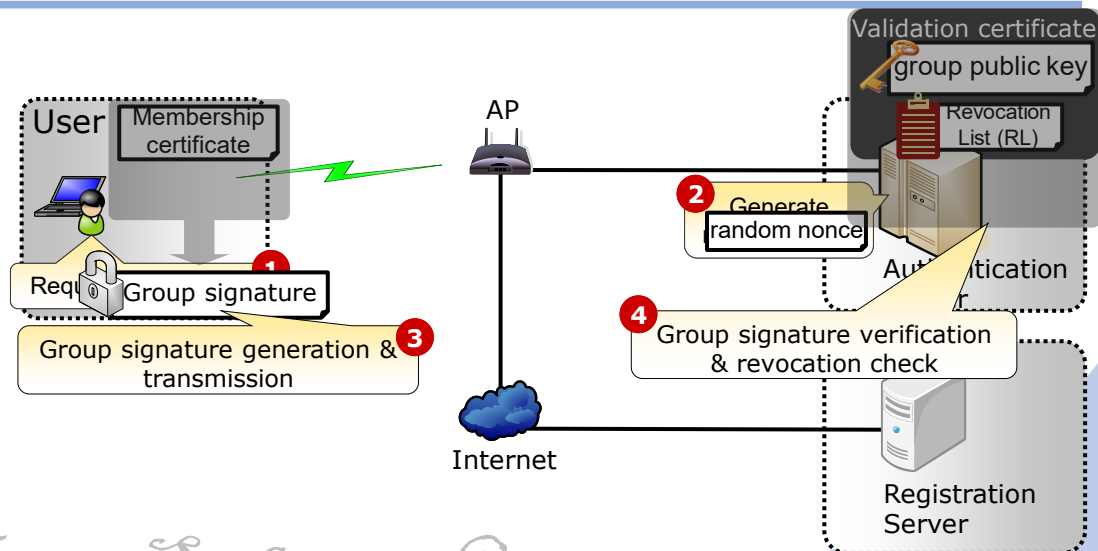


Group Manager
■ Manages the users

Amang Sudarsono @ 2020

6

EAP-TTLS/GS in IEEE802.1X Protocol



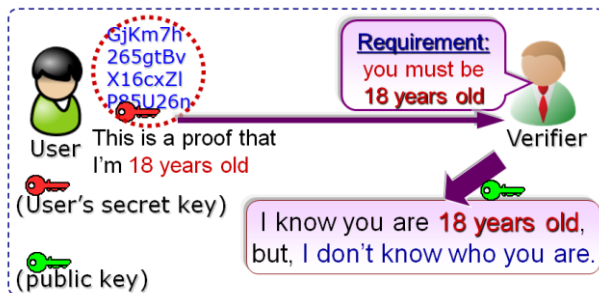
If the verification is valid, AP opens the port to allow user access the network.

Src: Amang Sudarsono, Toru Nakanishi, Yasuyuki Nogami, and Nobuo Funabiki, "Anonymous IEEE802.1X Authentication System Using Group Signatures", Journal of Information Processing, Vol. 18, pp. 63-76, March, 2010

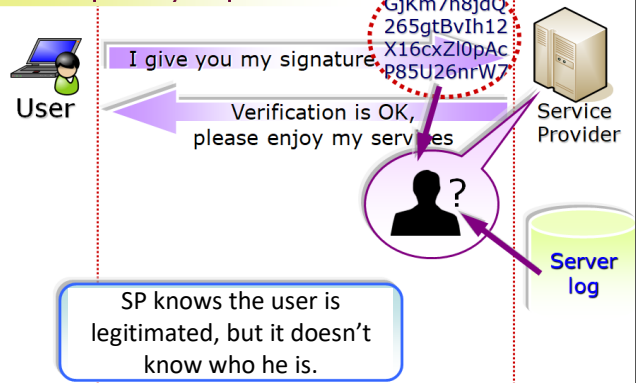
Anonymous Credential, Anonym. Auth

A user is allowed to prove the possession of particular attributes **anonymously**.

Similar to the group signature.



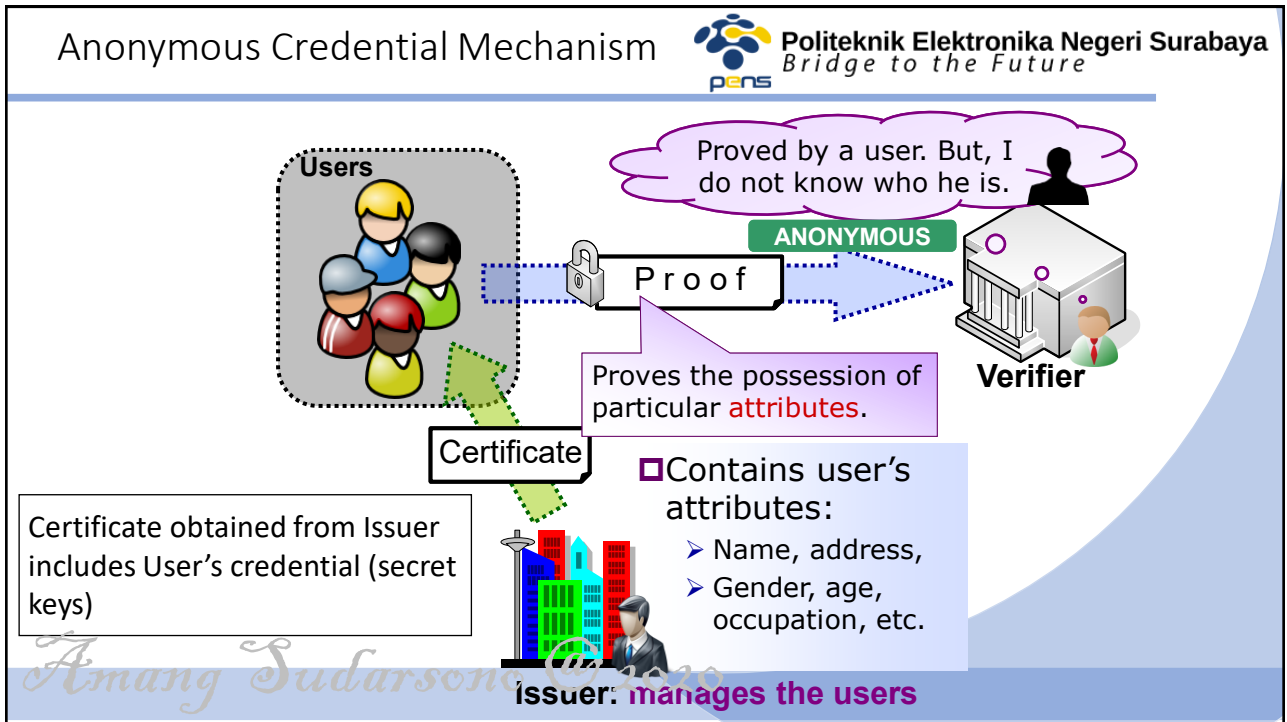
User's privacy is protected.



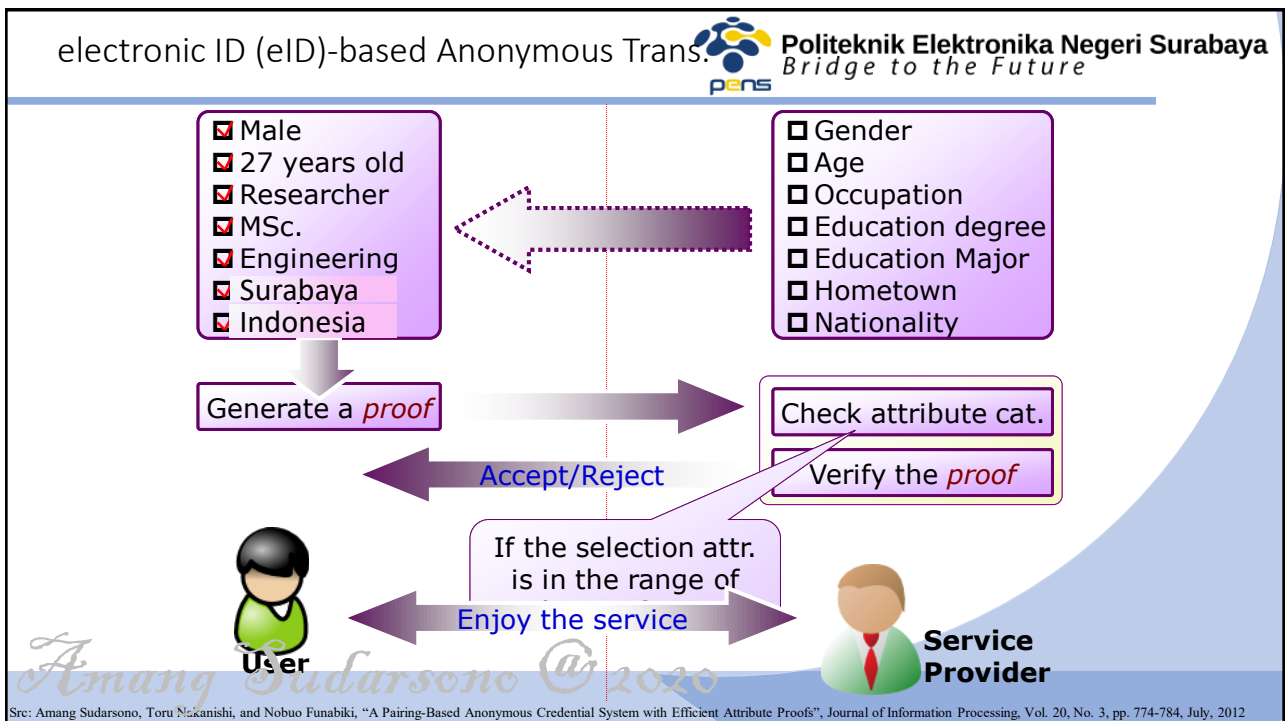
Anonymous Credential

Anonymous Authentication

Amang Sudarsono @ 2020



9



Src: Amang Sudarsono, Toru Makanishi, and Nobuo Funabiki, "A Pairing-Based Anonymous Credential System with Efficient Attribute Proofs", Journal of Information Processing, Vol. 20, No. 3, pp. 774-784, July, 2012

10

Crowdsensing of Travelling-User Behavior with Privacy Protection (Anonymous Credential)

Politeknik Elektronika Negeri Surabaya
Bridge to the Future

CHOOSING ROUTE
User start by choosing travel route with the assumption that the trip is planned before.
GOOGLE MAPS API

APPLICATIONS TRACKING
Track the applications usage. The 'tracking' is based on duration of applications usage and counter
ANDROID LIBRARY

CREATING BEHAVIOR
Create travelling behavior based on apps usage. Behavior creation is real time and changing based on apps usage.
APPLICATION CATEGORIZATION

DATA UPLOADING
Upload behaviors to the Server. Behavior creation doesn't occur once, thus it is uploaded with timestamp.
ANONYMOUS AUTHENTICATION

Anonymous User	Location	Running App.
526aew727mPZ (Male, 18 years old)	Lat, Long	Whatsapp, Camera
kjgS892Hb7Js7L (Female, 27 years old)	Lat, Long	Camera, Play Music

Behavior Data
Mikro Transisi at 17:09:46.272
Mikro Transisi at 17:03:56.585

Amang Sudarsono @ 2020

11

Crowdsensing of Group of Users Outdoor Activities with Privacy Protection (Anonymous Credential)

Politeknik Elektronika Negeri Surabaya
Bridge to the Future

walk, run, seat down or probably lay down, and the location

Acceleration Orientation

User 1 ... User n

Internet

Data Center Server

Collect acceleration and gyroscope data

Analyzing down on

The user n such as get location and activity status anonymously and pseudonymously.

Anonymous User	Location	Activity status
526aew727mPZ (Male, 18 years old)	Lat, Long	Berjalan
kjgS892Hb7Js7L (Female, 27 years old)	Lat, Long	Berjalan

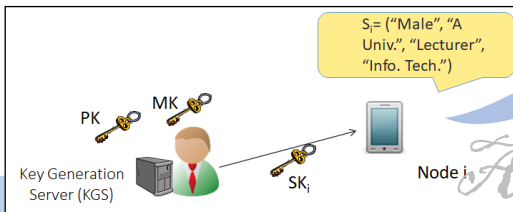
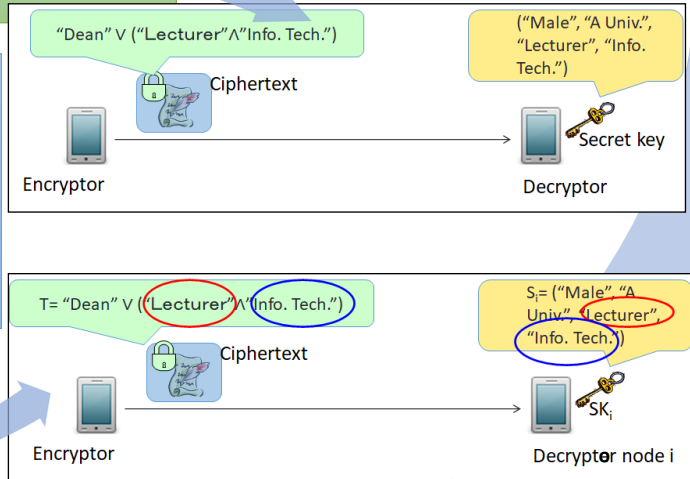
Amang Sudarsono @ 2020

12

Ciphertext Policy Attribute-Based Enc.

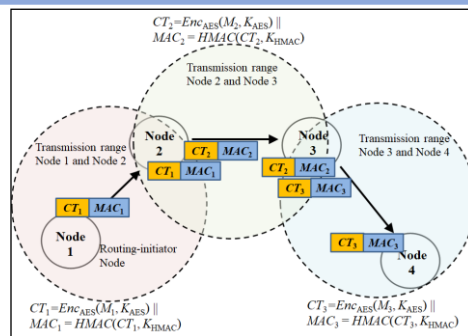
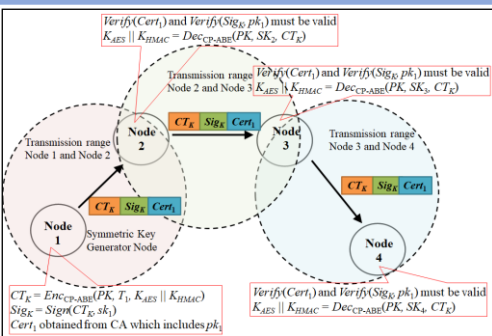
- Ciphertext has a policy of attributes (logical formula of attributes).
- Only user with satisfying attributes can decrypt it.

- **[Setup]** In advance, Key Generation Server (KGS) generates Public Key (PK) and Master Key (MK).
- **[KeyGen]** KGS generates each node i 's Secret Key (SK_i) associating with the attributes S_i .
- **[Enc]** Given PK, a policy of attributes T , and plaintext, generate the ciphertext.
- **[Dec]** Given SK_i and the ciphertext, extract the plaintext, if the attributes S_i satisfies policy T .



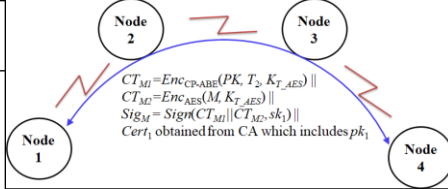
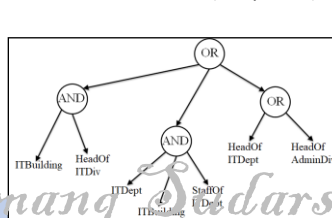
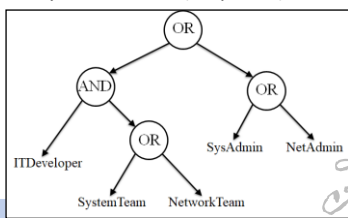
13

Secure Data Exchange in Wireless Delay Tolerant Network



Symmetric key distribution (1st phase)

Path establishment (2nd phase)

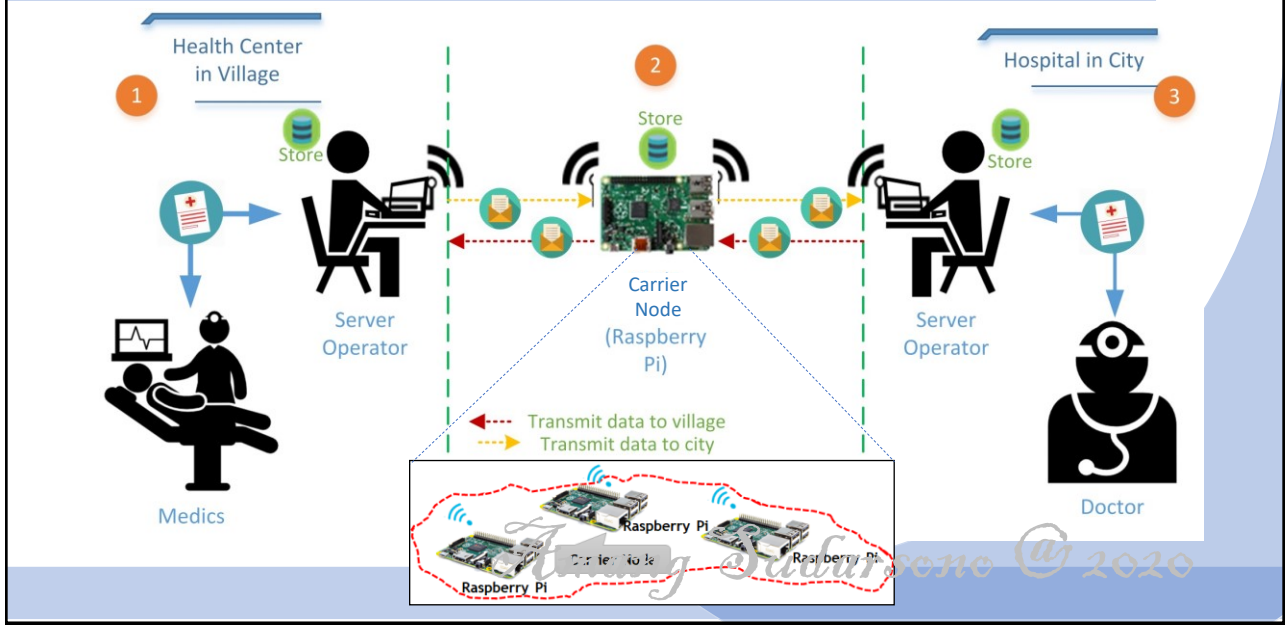


Content data transfer (3rd phase)

Src: Amang Sudarsono and Toru Nakanishi, "A Secure Data Exchange System in Wireless Delay Tolerant Network Using Attribute-Based Encryption", Journal of Information Processing, Vol. 25, pp. 234-243, 2017.

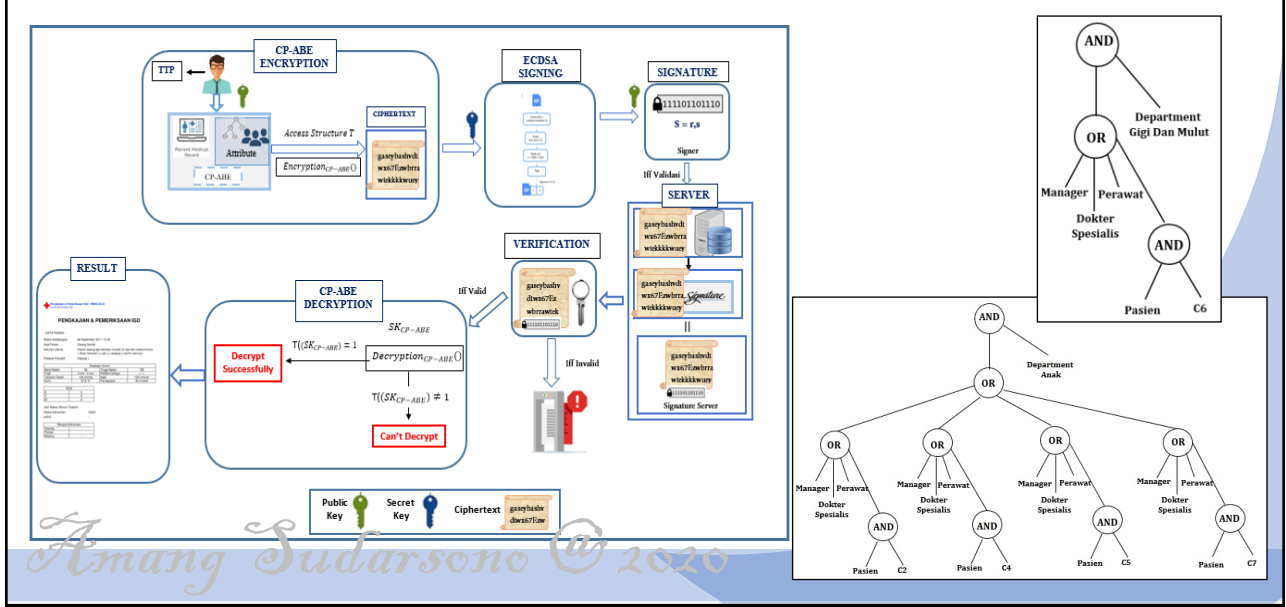
14

Secure Data Exchange in Wireless DTN (cont...)

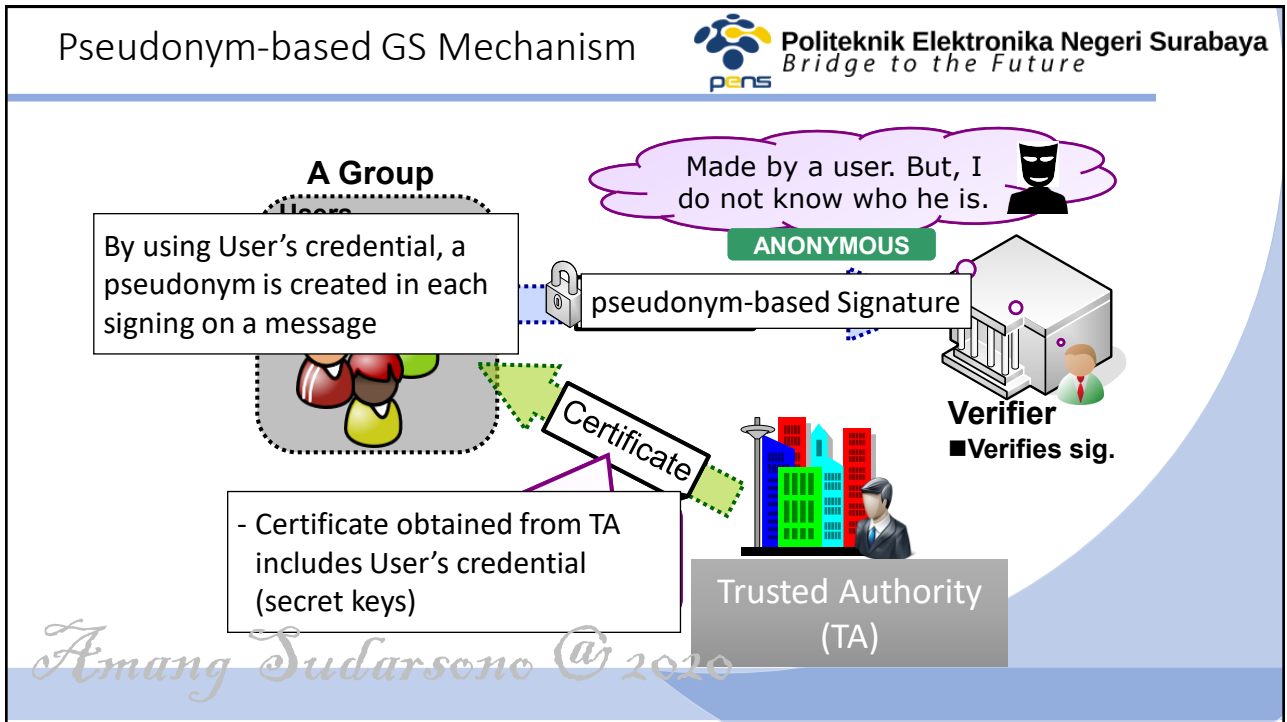


15

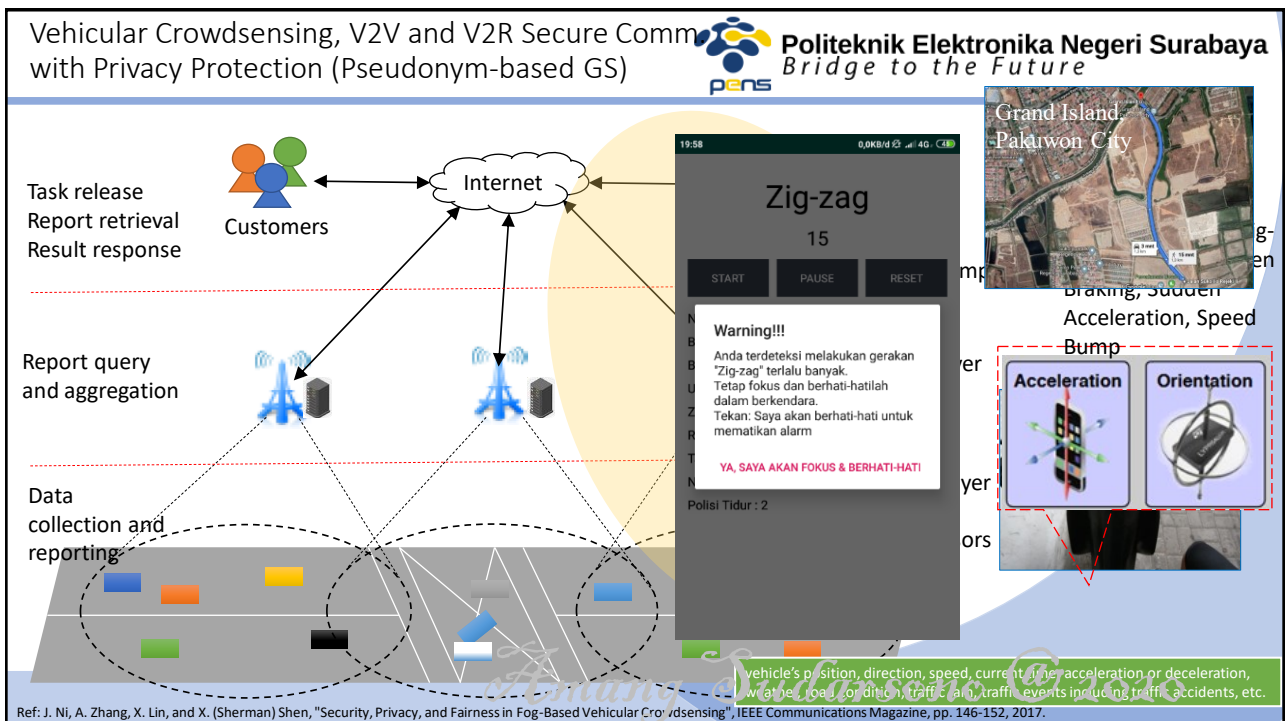
Secure Data Access for e-Health Monitoring using CP-ABE



16



17



18

Thank you....

Amang Sudarsono © 2020