Designing a Public Key Infrastructure for a National Healthcare Service

Cil Hardianto Satriawan / 13508061
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
if18061@students.if.itb.ac.id

Abstract: The expanding sophistication and scope of the internet means that an increasingly significant proportion of important communication, be that of individuals or businesses, is being conducted by digital means through the internet. In this paper, a secure web-based implementation of a national healthcare service for Indonesia is proposed. A public key infrastructure is designed, with a governing agency acting as a certificate authority in the issuance of new certificates to individuals and healthcare businesses. Communication between parties is cryptographically secured; medical claims are digitally signed to ensure authenticity, integrity, and legal non-repudiation. Prior implementations are discussed, specifically that of Australia's Medicare. Finally, concerns regarding individual rights to privacy and system limitations are discussed.

Key Words: *public key infrastructure, national healthcare, digital signature, digital certificate, security, cryptography, universal health care*

I. Introduction

In an era of expanding internet usage and sophistication, Indonesia lags behind developed nations and even its neighbours in terms of internet application at the national level. Our various neighbours have at different points of time developed web-based systems to accommodate electronic voting[], national healthcare[], financial management[], etc. This is despite significant growth in the usage of mobile broadband in Indonesia as compared to the global average, which would indicate that a steadily growing proportion of our society is online.

Web-based, digital systems to address matters of public importance have been shown to be beneficial as compared to traditional pen-and-paper implementations. Benefits include; wider distribution of information, significantly faster information distribution, scaling of costs, and the reduction of physical and environmental costs. A web-based, digital system to address national policies would also have unique benefits (and disadvantages) when applied in Indonesia, and by extension, developing nations, including; bypassing certain levels of bureaucracy, hence reducing the opportunity for corruption and increasing response speed of the system, reducing the total carbon footprint from usage of a pen-and-paper system, and easier distribution of information in a maritime nation.

Currently, Indonesia has a vast network of public hospitals, with digitised registration and management. Utilising this network, a centralised national healthcare service could be implemented to leverage the advantages web-based systems confer. In such a system, individuals would register to the service electronically and receive healthcare from similarly registered healthcare services. Healthcare services constitute public hospitals, for which registration would be obligatory, and private healthcare individuals or institutions that wish to join the service and apply for government reimbursement of services rendered to patients subscribed to the program. An individual may issue a claim to reimburse certain medical services directly to the government; specialist services, for example, may be exempted from direct reimbursement from the healthcare service. Similarly, private healthcare services may issue reimbursement claims for the services that fall under the reimbursement program; for instance, general healthcare (dokter umum) may fall under the reimbursement agreement but specialist services may not. A system of centralised patient records could then be collected and compiled from data submitted from the various registered healthcare services.

The main concern of such a system would be data security; the governing agency responsible for receiving and reimbursing claims from individuals and healthcare services would need to be certain of the authenticity of the subject, i.e. the individual registered is indeed the recipient of the healthcare claimed, or the healthcare service applying for reimbursement is indeed authentic. In the opposite direction, individuals and healthcare services need to be sure information distributed from the governing agency is authentic. The security infrastructure most suited to these requirements is the public key infrastructure, that implements assymetric key encryption to secure data.

II. Theory

Assymetric key encryption is a means of encryption whereby a pair of keys are used, in contrast to the more traditional symmetric key encryption. In symmetric key encryption, the same key is used for encryption and decryption of data. In assymetric key encryption, the public key is made public and widely and freely distributed, whereas the private key is never distributed and is kept secret. Given a key pair, data encrypted with the public key can only be decrypted with its private key; conversely, data encrypted with the private key can only be decrypted with its public key. This characteristic is used to implement encryption and digital signature. The advantages of using public key encryption are simplified key distribution, digital signature, and long-term ecnryption.

2.1 Public Key Encryption and Digital Signature

The main idea behind public key encryption is the problem of large prime factorisation. The difficulty of factoring the product of large primes is exploited to obtain two keys; a widely and freely distributed public key, which is analogous to a lock, and a secret private key, analogous to a key. The most widely used implementation of public key encryption currently used is the Rivest-Shamir-Adleman (RSA) algorithm. The following is a worked example of using the RSA algorithm for encryption and decryption, with values artificially small as compared to real-world examples, and without the implementation of padding:

1. Choose two distinct prime numbers, such as

   $p = 61$ and $q = 53$

2. Compute $n = pq$ giving

   $$n = 61 \times 53 = 3233$$

3. Compute the totient of the product as $\varphi(n) = (p - 1)(q - 1)$ giving

   $$\varphi(3233) = (61 - 1)(53 - 1) = 3120$$

4. Choose any number $1 < e < 3120$ that is coprime to 3120. Choosing a prime number for e leaves us only to check that e is not a divisor of 3120.

   Let $e = 17$

5. Compute d, the modular multiplicative inverse of e (mod $\varphi(n)$) yielding

   $$d = 2753$$

The **public key** is ($n = 3233$, $e = 17$). For a padded plaintext message m, the encryption function is

$$c(m) = m^{17} \mod 3233$$

The **private key** is ($n = 3233$, $d = 2753$). For an encrypted ciphertext c, the decryption function is

$$m(c) = c^{2753} \mod 3233$$

For instance, in order to encrypt $m = 65$, we calculate

$$c = 65^{17} \mod 3233 = 2790$$

To decrypt $c = 2790$, we calculate

$$m = 2790^{2753} \mod 3233 = 65$$

Suppose Alice uses Bob's public key to send him an encrypted message. In the message, she can claim to be Alice but Bob has no way of verifying that the message was actually from Alice since anyone can use Bob's public key to send him encrypted messages. In order to verify the origin of a message, RSA can also be used to sign a message.

Suppose Alice wishes to send a signed message to Bob. She can use her own private key to do so. She produces a hash value of the message, raises it to the power of d (modulo n) (as she does when decrypting a message), and attaches it as a "signature" to the message. When Bob receives the signed message, he uses the same hash algorithm in conjunction with Alice's public key. He raises the signature to the power of e (modulo n) (as he does when encrypting a message), and compares the resulting hash value with the message's actual hash value. If the two agree, he knows that the author of the message was in possession of Alice's private key, and that the message has not been tampered with since.

2.2 Public Key/Digital Certificate

A public key /digital certificate is an electronic document that uses the digital signature of a trusted third-party (usually a Certificate Authority, see section below) to bind a public key with an identity, such as a name, address, or personal identification number. The certificate can then be used to verify that a public key belongs to an individual.

In the X.509 standard, the contents of a digital certificate contain a; serial number, subject, signature algorithm, signature, issuer, valid-from (the date the certificate is valid from), valid-to (expiration date), key-usage, public key, thumbprint algorithm (the algorithm used to hash the public key certificate), thumbprint (the hash of the public key certificate).

2.3 Public Key Infrastructure

A Public Key Infrastructure (PKI) is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates. In this arrangement, specific public keys are bound to their respective user identities by means of a certificate authority. This binding is established through a registration and issuance process, with implementations that vary according to the nature of the system involved. This binding is conducted in a way that ensures authentication and non-repudiation. The legal status of this binding varies according to the laws applicable to the region involved.

A public key infrastructure typically is comprised of the following components:

- A certificate authority (CA) responsible for issuing and verifying digital certificates.
- A registration authority (RA) which verifies the identity of users requesting information from the CA.
- A central directory, a safe location in which to store public-private key pairs and digital certificates.
- A certificate management system, for managing active/expired certificates
- A certificate policy, a set of rules governing how certificates are standardised, their expiry date, etc.

Although this paper considers the above definition of a PKI, there exist other schemes whereby certificate issuance and verification are distributed (Web of Trust) and where public keys need not be bound to specific users (Simple Public Key Infrastructure).

A public key infrastructure is responsible for providing:

- Encryption and/or sender authentication of sent data, be it messages and e-mail (OpenPGP) or documents.
- Authentication of users to applications (smart card/USB dongle logon, SSL client authentication).
- Bootstrapping secure communication protocols such as Secure Socket Layer (SSL) and Internet Key Exchange (IKE). In both instances, the initial setup of a secure channel for communication uses assymetric key encryption, whereas the actual communication employs the faster symmetric key method.
- The issuance of mobile digital certificates to location-independent telecommunication devices such as mobile phones.

A public key infrastructure is often the choice of security implementation for nation-wide systems such as electronic voting and healthcare services, an example of which is the Australian National Healthcare Service, Medicare.

III. Case Study: Australian Medicare

Medicare is a publicly funded universal health care scheme in Australia. Medicare has existed in various forms from its inception in 1975. In its current form, Medicare provides an online service for healthcare individuals to issue reimbursement claims to the governing agency involved. There are a number of identifiers the system can recognize, illustrated in figure 1 below.

Aside from individuals seeking medical reimbursement, Medicare also identifies healthcare providers, in two categories, healthcare individuals and healthcare organizations. The hierarchy of sub-division within the organization is also recognized; various sub-division may request to be identified as individual healthcare providers under a larger healthcare organization. An example is provided in fig. 2 of the Sydney Hospital.

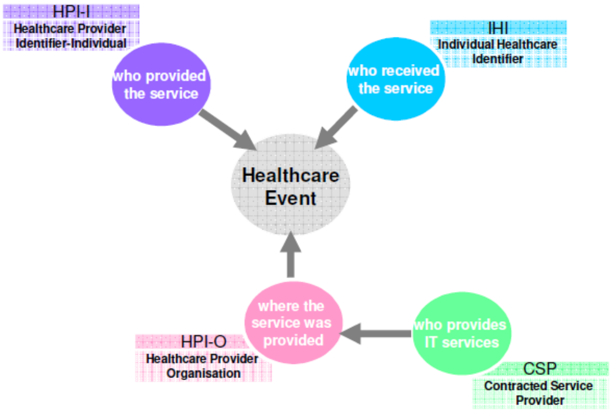

HPI-I
Healthcare Provider Identifier-Individual
who provided the service
IHI
Individual Healthcare Identifier
who received the service
Healthcare Event
where the service was provided
who provides IT services
HPI-O
Healthcare Provider Organisation
CSP
Contracted Service Provider

fig. 1 relationship between identifiers in a Healthcare Event

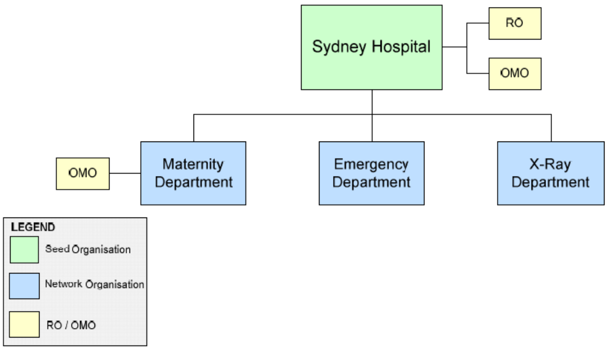


fig. 2 organisation hierarchy of healthcare provider

Healthcare individuals, providers, and provider organizations differ in their usage of the system and the way they interact with it. Individuals may access the system directly through a web browser personally, or if a home/mobile connection is unavailable, they can access the system through a computer provided at the Medicare Services Office (MSO). Healthcare providers, in addition to the choices available to individuals, may also access the system through specialized software vendors, through which they can input patient data to the governing agency. The information collected through this method is further compiled to generate an individual's complete medical history. These processes are illustrated in figure 3 below.

Finally, the service provides certification management for the governing agency involved. Specifically, certificate expiration is addressed through 5-year renewing of all certificates of the parties involved; once the CA renews its public key, a transmission to all individuals and healthcare providers is sent to update the public key information pertaining to the CA.

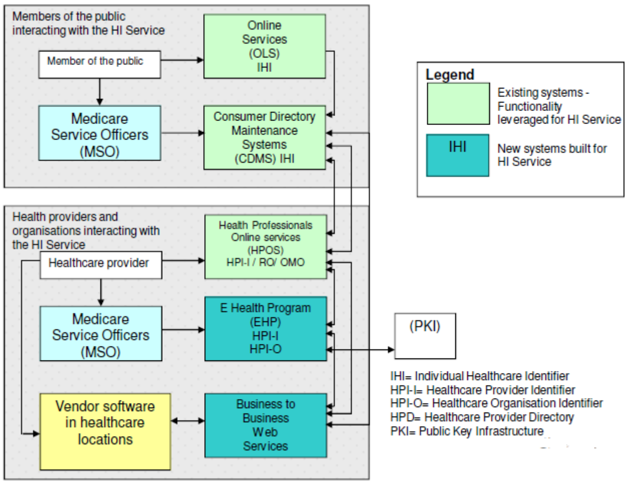

Members of the public interacting with the HI Service
Member of the public
Online Services (OLS) IHI
Medicare Service Officers (MSO)
Consumer Directory Maintenance Systems (CDMS) IHI
Legend
Existing systems - Functionality leveraged for HI Service
IHI
New systems built for HI Service
Health providers and organisations interacting with the HI Service
Healthcare provider
Health Professionals Online services (HPOS) HPI-I / RO/ OMO
Medicare Service Officers (MSO)
E Health Program (EHP) HPI-I HPI-O
(PKI)
IHI= Individual Healthcare Identifier
HPI-I= Healthcare Provider Identifier
HPI-O= Healthcare Organisation Identifier
HPD= Healthcare Provider Directory
PKI= Public Key Infrastructure
Vendor software in healthcare locations
Business to Business Web Services

fig. 3 Medicare systems service

IV. Design and Analysis

In order to design a public key infrastructure to secure the proposed national health care service, a number of assumptions regarding the structure of the service, its operation and functionality need to be made. In this case, the example of Australia's Medicare is taken as a template for the design of the health care service, with modification in parts to adhere to the requirements of the system:

4.1 Actors/Identifiers

There are 4 unique actors/identifiers considered by the system; Individuals, Providers, Provider Organizations, and the Governing Agency that acts as the Certificate Authority. The relationship between actors in the certification process is illustrated in fig 4.

The actors interact with the PKI in different ways, depending on the type of actor and the method invoked by the actor. For example, individuals interact with the system to claim reimbursements and to check the status of their medical record. Healthcare providers interact with the system to input medical data, make reimbursement claims, etc. In each case, actors must follow the procedure outlined in Appendixes A, B, and C attached at the end of the document in issuing and using digital certificates and signatures.

4.2 Security

In order to ensure secure communication between all parties, the system must be configured at the beginning; firstly, a distinction is made between a governing agency, which receives and processes claim requests, and the certificate authority, which generates and stores the digital certificates of all actors requesting and providing healthcare.

The certificate agency, firstly, generates a public-private key pair for its own use, i.e. to create a digital signature and digital certificate for itself.

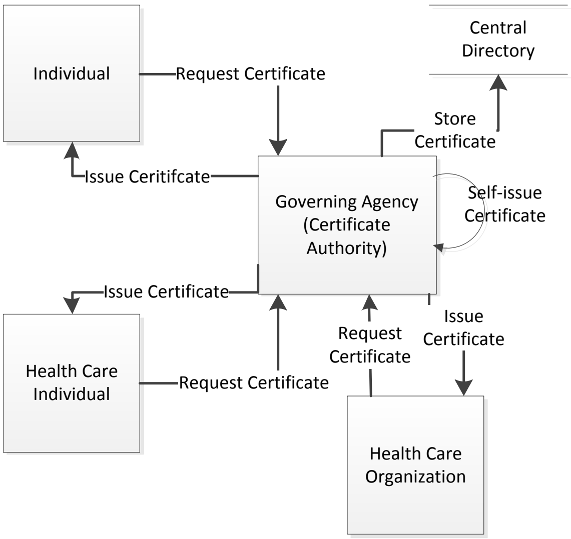


fig. 4 relationship between actors

Secondly, when an individual / healthcare provider / healthcare organization registers for the service, the certificate authority verifies the request against personal identification or, in the case of providers, their medical license. A public-private key pair is then generated and a digital certificate made. A physical copy of the certificate is sent to the actor, and the private key, embedded in a USB dongle or similar smart card, is sent separately.

When issuing a claim, the claimant signs the claim with their digital signature before sending it to the certificate authority. The CA verifies the signature of the claimant, and if found to be authentic, sends it over to the governing agency, who then processes the claim.

Finally, the governing agency sends a response, signed with the digital signature of the governing agency, verified by the CA, to the claimant in question. The claimant then verifies the signature and reads the content of the response.

V. Limitations

Despite the significant benefits, there remain substantial hurdles for implementation in Indonesia. As a matter of national importance, an over-reliance on foreign expertise and foreign technology in designing and implementing the system would be inadvisable. Local expertise regarding the implementation of a system of such magnitude remains scarce. Furthermore, a central directory of certificates would be vulnerable to physical attack, whereas a distributed cloud system of such scale would rely on foreign technology, or utilise servers physically located elsewhere in the world.

While it is true that internet penetration is rapidly growing in Indonesia, a majority of the population is still offline.

Implementation of a web-based national healthcare service would hence raise concerns of inequality and unfair distribution of taxpayer money. For instance, internet penetration in remote areas such as the Kalimantan heartlands, vast swaths of East Indonesia, and Papua, remain insubstantial. A workaround would be to maintain and facilitate online medical claim centers in public hospitals or other public venues, such as district offices (kantor kelurahan). In this way, prospective individuals may register and claim medical reimbursement from these centers. Obviously, this workaround removes some of the benefits; the reintroduction of "middle men" may introduce additional opportunities for corruption from local bureaucrats or hospital administrators.

Another concern deals with civil rights and individual rights to privacy. The storage online of personal, individual medical records is of concern, as government officials may be able to access such data. Furthermore, it is an open question in Indonesia whether there are laws regarding the protection of personal digital information, and if such laws can be enforced.

Finally, it is unclear whether such a large undertaking would be feasible from a budget standpoint, as the cost would be potentially astronomical given current conditions. Points to consider include, but are not limited to; the absence of adequate network infrastructure in many parts of Indonesia, the potentially steep learning curve of using the system to uninitiated users (given low internet penetration), the possibility of corruption throughout development, which may or may not compromise the final product.

VI. Conclusion

Although a nation-wide health care service utilizing the internet may be a pipe dream at this point, considering the tremendous hurdles to overcome, it is not entirely unrealistic. Given the current growth of internet usage in Indonesia through mobile broadband, it is possible that internet usage will be evenly distributed by the end of the decade.

Either way, the implementation of a web-based health care service has the potential to bring affordable health care to a large proportion of the population at a reasonable speed and without too much “middle man” intervention. As demonstrated, a secure infrastructure is possible to implement concurrent to the implementation of the service, and the infrastructure proposed here has already been implemented successfully in neighbouring nations.

REFERENCES

Curry, Ian, Entrust Technologies, “Getting Acquainted With Entrust/Solo and Public-key Cryptography”, version 1.0, July 1997.

Branchaud, Marc, “A Survey of Public-key Infrastructures”, Department of Computer Science, McGill University, Montreal, 1997.

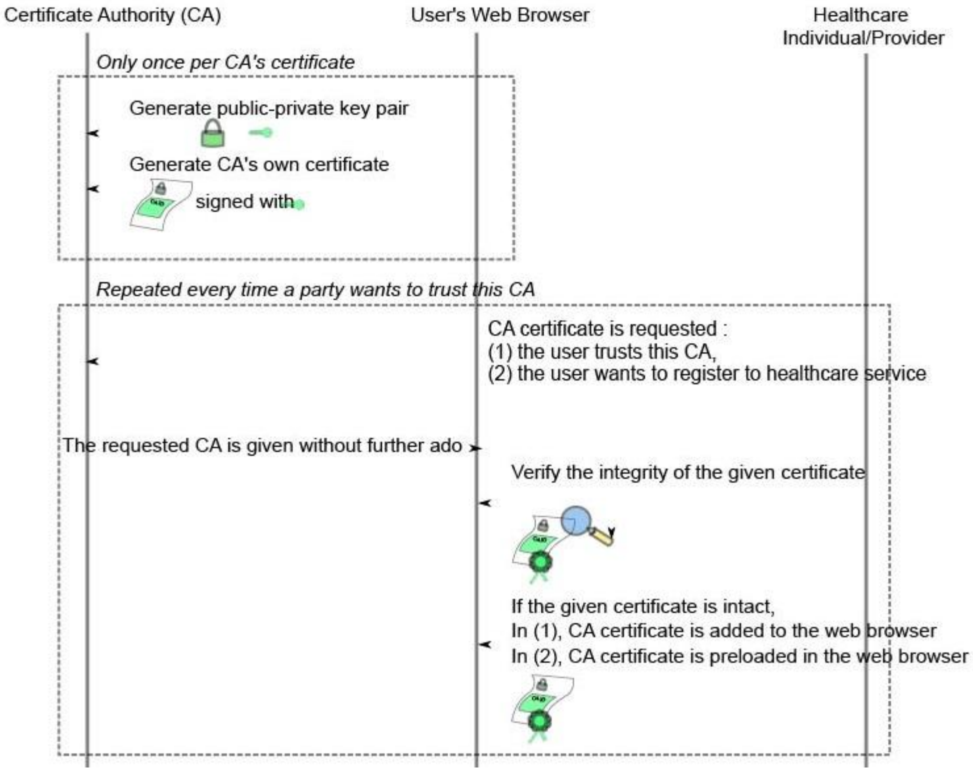
RSA, “Intro to PKCS Standards”, http://www.rsasecurity.com/solutions/developers/whitepapers/IntroToPKCSstandards.pdf.

PERNYATAAN

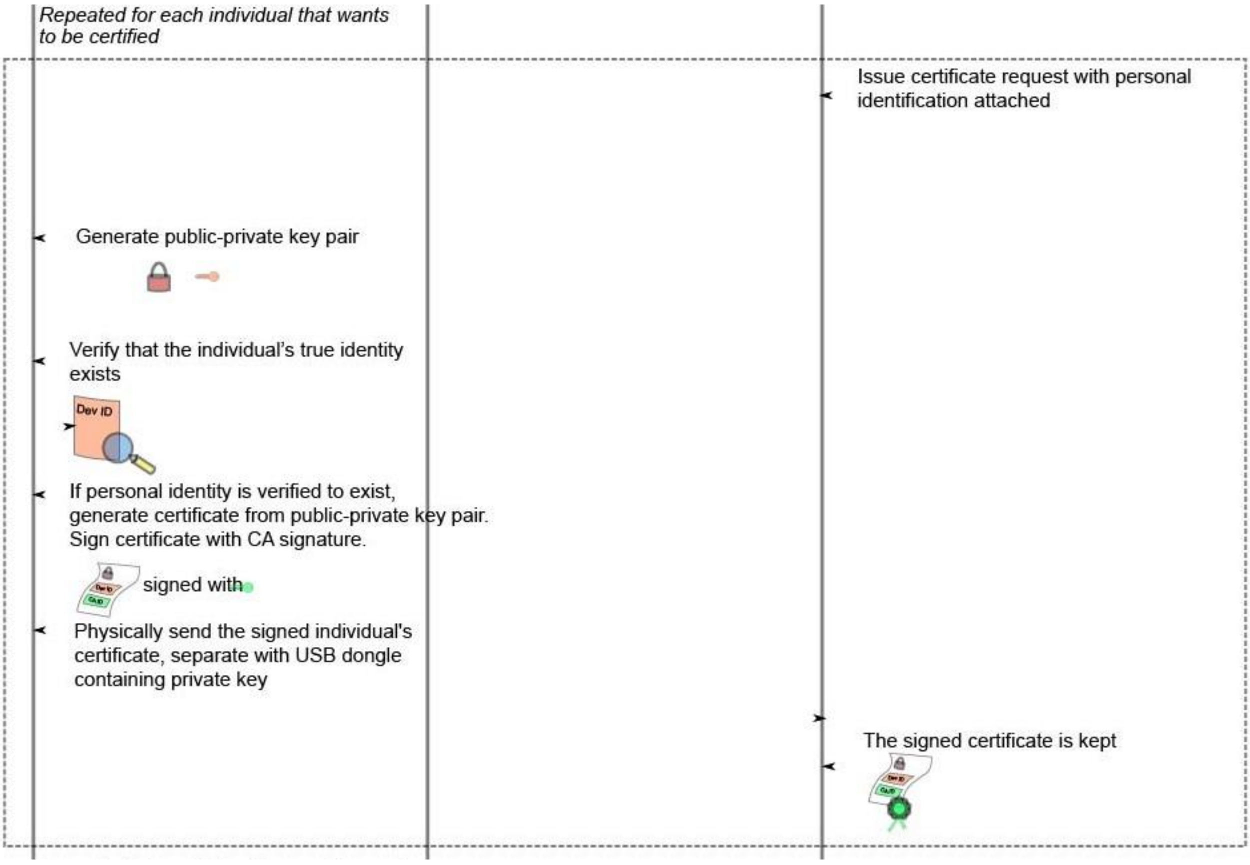
Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 15 Mei 2014

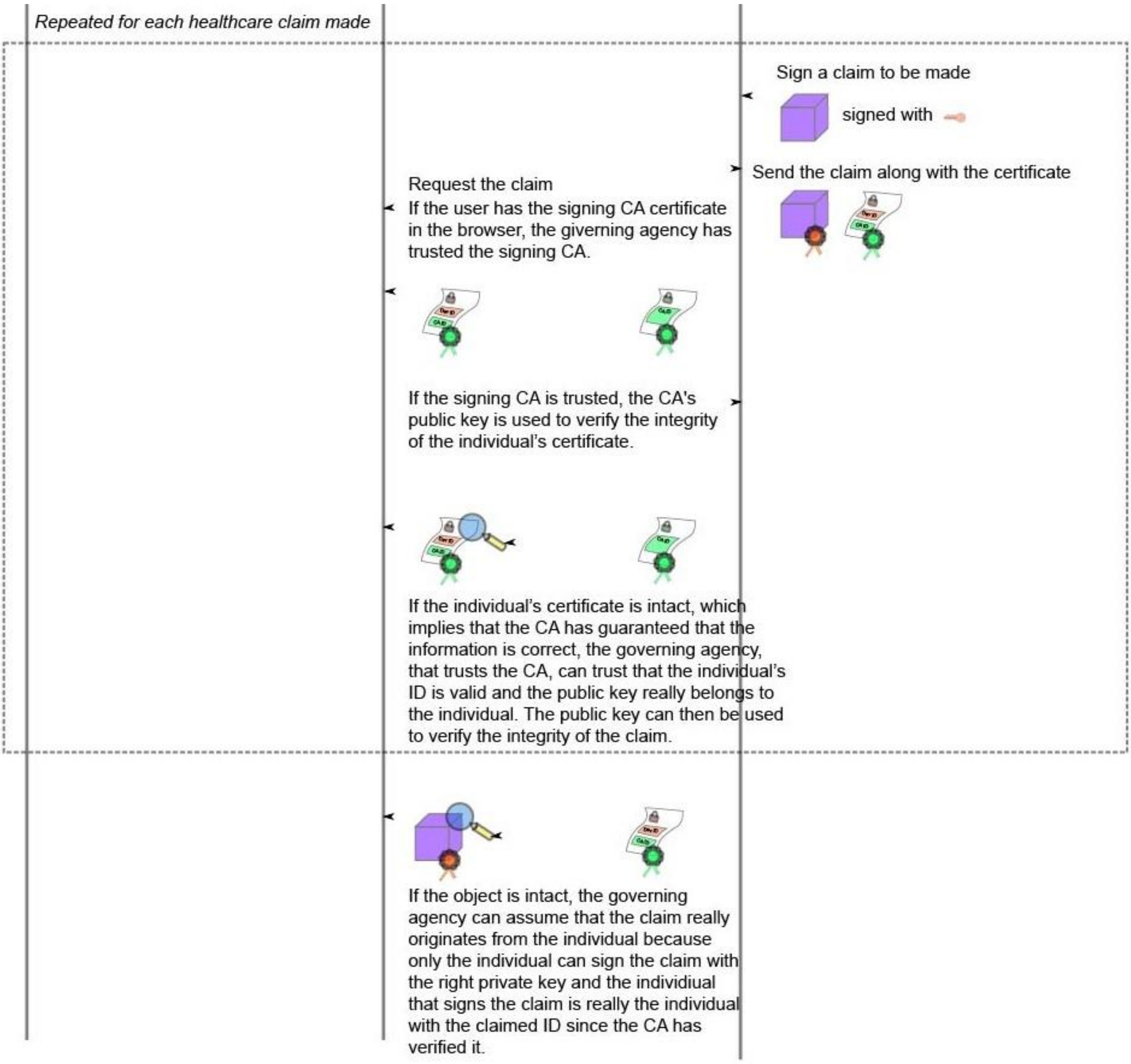
Cil Hardianto Satriawan 13508061


Certificate Authority (CA)
User's Web Browser
Healthcare Individual/Provider
Only once per CA's certificate
Generate public-private key pair
Generate CA's own certificate
signed with
Repeated every time a party wants to trust this CA
CA certificate is requested :
(1) the user trusts this CA,
(2) the user wants to register to healthcare service
The requested CA is given without further ado
Verify the integrity of the given certificate
If the given certificate is intact,
In (1), CA certificate is added to the web browser
In (2), CA certificate is preloaded in the web browser

Appendix A Ceritification request


Repeated for each individual that wants to be certified
Issue certificate request with personal identification attached
Generate public-private key pair
Verify that the individual's true identity exists
Dev ID
If personal identity is verified to exist, generate certificate from public-private key pair. Sign certificate with CA signature.
signed with
Physically send the signed individual's certificate, separate with USB dongle containing private key
The signed certificate is kept

Appendix B Issuing certificate


Repeated for each healthcare claim made
Sign a claim to be made
signed with
Send the claim along with the certificate

Request the claim
If the user has the signing CA certificate in the browser, the giverning agency has trusted the signing CA.

If the signing CA is trusted, the CA's public key is used to verify the integrity of the individual's certificate.

If the individual's certificate is intact, which implies that the CA has guaranteed that the information is correct, the governing agency, that trusts the CA, can trust that the individual's ID is valid and the public key really belongs to the individual. The public key can then be used to verify the integrity of the claim.

If the object is intact, the governing agency can assume that the claim really originates from the individual because only the individual can sign the claim with the right private key and the individiual that signs the claim is really the individual with the claimed ID since the CA has verified it.

Appendix C Reimbursement claim procedure and verification