Digital Signature in Education Sector

Ranindya Paramitha
Informatic Department
STEI, Institut Teknologi Bandung
Surakarta, Indonesia
13516006@std.stei.itb.ac.id

***Abstract*—Digital data and messages is very common in this modern word. To assure integrity and authenticity of digital data, digital signature could be utilized to sign and verify those data/ messages. Digital signature is a cryptographic primitive which is used to sign digital messages. Many industries have taken benefits from digital signature, including education sector. Education sector is a specific sector which comprises all education-related matters. There are some processes in education sector which could be optimized using digital signature, including student application, transcripts and certificates signing, online permission slips, also announcement and document distribution. Using digital signature, education sector gains benefits such as increased security, reduced time and cost, paperless system, more comfortable and easy to use system, also streamlined processes.**

Keywords—education sector; digital signature;

I. Introduction

In this modern word, more and more data are getting digitalized in order to ease data storing and distribution. Digital data and message could be duplicated easily. For these digital data and messages, traditional signature accuracy for determining message authenticity is not very high anymore. This is why digital signature technology is needed. Education sector is one sector that has may data to be stored. There are also many announcement messages need to be signed before being distributed. Considering these, digital signature could be beneficial to optimize some processes in education sector.

II. Theories

A. Education

According to Cambridge Dictionary in reference [4], education means the process of teaching or learning, especially in a school or college, or the knowledge that you get from a high school/college. Thus education sector is a sector that comprises all education-related matters, including education system, teaching strategies, admission and graduation system, etc.

B. Public Key Cryptography

According to Merriam-Webster dictionary in reference [3], cryptography means the enciphering and deciphering of messages in secret code or cipher. Cryptography itself has two types: symmetric and asymmetric cryptography. Asymmetric cryptography is also known as public key cryptography.

Public key cryptography uses two different keys, one for encryption and one for decryption. Public key is a key which is published to public, while private key is confidential and only known by the owner. In common public key encryption, the plain text message is encrypted using receiver's public key and becomes cipher text. On the receiver side, the cipher text is decrypted using the receiver's private key. This cryptography assure confidentiality and integrity of a message.

C. Digital Signature

Digital signature is a cryptographic primitive which is fundamental in authentication, authorization and nonrepudiation [1]. Digital signature is basically a signature for digital data. Digital signature comes in the form of cryptographic value which depends on message content and key value. There are two ways to sign a message: encrypt the message or use the combination of public key cryptography with hash function.

1) Encrypt the message

a) Using symmetrical cryptography

Symmetrical cryptography assures authenticity of message because only sender and receiver of an encrypted message should know the key to decrypt it. However, digital signature using this could not assure non-repudiation of the message.

b) Using public key cryptography

The sender encrypts the message using his/her own private key before sending it to the receiver. On the other side, the receiver could validate the message by decrypting it using sender's public key. This idea was found by Diffie-Hellman. Using public key cryptography in digital signature assure both confidentiality and authenticity of the message. Two public key cryptography algorithm that is commonly used in digital signature are RSA and El-Gamal.

2) Combination of public key cryptography - hash function

In some cases, confidentiality of the message is not priority, and digital signature is needed only to assure authenticity of the message. For these cases, combination of public key cryptography and hash function could be used as shown in Fig. 1.

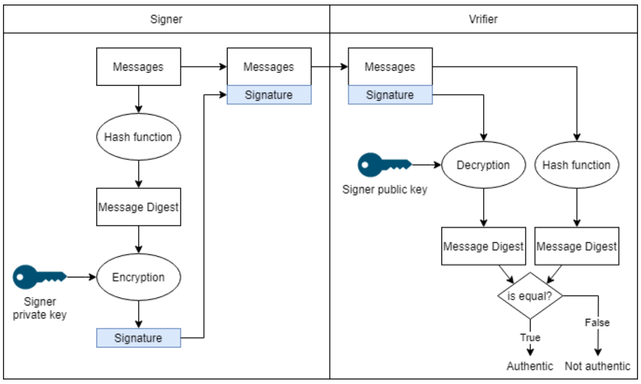

Fig 1. Digital Signature Combination Work Flow [2]

The signer of message should pass the message through a hash function to get its message digest. Then the message digest is encrypted using signer's private key to get the unique signature. This signature is embedded on the message and the combination of those two is then sent to the receiver.

The receiver or verifier who receives the message with signature on it then separates the signature and the message. He/she decrypts the signature using the signer's public key to get a message digest. The message is also processed using a hash function (the same function with the one used by the signer) to get another message digest. These two message digest are then compared. If both are equal, the message is authentic.

DSA (Digital Signature Algorithm) is an algorithm that was set as Digital Signature Standard. Unlike RSA, which has symmetrical signature and verification algorithm, DSA has different algorithm for those two steps [2].

D. *Security Properties Protected by Digital Signature*

Digital signature utilization could increase security of documents. There are some security properties mentioned in this paper which could be protected by digital signature usage.

1) *Confidentiality*

Confidentiality is a property that means a document or message is not available for unauthorized agents [9]. Digital signature that could protect this property are the ones using symmetric key and public key cryptography (assuming that public key are known by authorized people).

2) *Integrity*

Integrity means that a document or message should be protected from any unauthorized tampering effort. When a document/ message that arrive on receiver side is completely the same with the one that was sent by the sender, we could say that the integrity is protected. All digital signature could protect this property, because when a document is tampered, either the document could not be decrypted or the message digests would be different.

3) *Authenticity*

Authenticity is a property that prove someone's claim of his/her identity [10]. If a signed document is verified on the receiver side, we could conclude that the encryption key is valid. Valid encryption key is only owned by the signer, which concludes that the signer is not making a false claim about his/her identity. Either cryptographic or combined hash-public key cryptography digital signature could protect authenticity of the document signer.

4) *Non-Repudiation*

Non-repudiation means that anybody could not repudiate their action on something. Using digital signature, someone who has digitally signed a document would not be able to repudiate that action. This is because a digital signature is unique and when the signature could be verified using decryption key, it proves that only the one who has the matching encryption key that could sign the document.

III. Digital Signature in Education Sector

Digital signature could be beneficial for industry sectors, including education sector. There are some ways where digital signature could be used to give some benefits for education sector.

A. *Education Sector Processes to Be Upgraded*

Here are some processes which could be upgraded using digital signature technology:

1) *Student Application* [5,6]

Student enrolment process is an annual process which student candidates are needed to submit their data to apply to their desired school or university. These days, many schools and universities are utilizing online form and application for their applicants. However, this approach needs effort to validify applicants' data every time the data is distributed among departments for administration purposes, which is very time consuming to be done manually. This is where digital signature could take part. On the first enrollment process, the application should be given a digital signature, which then embedded on it. So every time it is distributed, the receiver could verify whether the application is authentic or not.

2) *Transcript or Certificates Signing*

Every time students want to apply to universities or companies, they need to request signed and sealed transcript or certificates from their previous institution. This process definitely takes time and involves cost if is done manually. Digital signature could help to make this process more efficient.

Every student's documents should be digitally signed by the institution that created them. Once a document is digitally signed, it could be used to apply to any other institutions which would verify the signature. If the document is tampered, message digest of the signature and the content would be different, so the institution could reject the document as it is not authentic. This way could reduce time and cost of transcript signing [5].

3) Online Permission Slips

Permission slip is a document used in US education system which is created by a school or institution to ask parents' authorization for students to travel under their care. Permission slips are usually given to parents long before the event itself, which would be troublesome if it is lost and parents have to search for it at the last minute [7]. This problem could be reduced using digital signature technology.

Institutions like schools could change to online permission slip. They could send it to parents using special application, which would ask parents to sign the permission slip. After the permission slip arrived at parents' side, the application would wait for parents' approval. When they approve (for example by giving their or their child data), the parent side application would sign the permission slip using parents' approval and send the signed permission slip back to the institution. On the institution's side, the application would verify the signature to show whether the permission slip is authentic or not.

4) Announcement and Document Distribution

In schools, universities, and other education institutions, administration is one crucial process to facilitate communication among departments and educational staffs, including students [7]. During this process, documents are very often used as media to transfer information and announcement. These days, most institution choose to use digital document than paper document. To avoid any document and announcement falsifications, digital signature could be used to sign and verify documents/ announcements. Digital signature using cryptography could even be used to assure confidentiality of documents and announcements.

For example, a dean should attach his/her digital signature to his/her announcement about students end year days off before distributing it to educational staffs and students. This way, if the announcement is tampered on the distribution process, the message digest would be different if it is verified on the receiver side. Therefore, nobody could tamper the announcement and .cause false information to spread.

Another example is when a university rector wants to share a confidential information to faculty deans. The rector could sign the information by encrypting it using his own private key and then share it to the deans. The deans would be able to get the information by decrypting it using the rector public key. If the information was tampered on the distribution process, the decrypted information would be messy and not-readable. The information also could not be spoofed along the way because it is encrypted. This way could be used assuming the rector public key is only known by the deans and other trusted agents.

B. Benefit of Using Digital Signature in Education Sector

Using digital signature in signing education-related documents brings some benefits for education sector itself. It gives benefit not only for the institution, but also for students and educational staffs.

1) *Reduce cost* [5,8]

Using digital documents with digital signature would reduce paper and printing cost.

2) *Reduce time* [8]

Traditional paper documents need to pass through many steps. It needs to be printed, signed manually, and then sent inside secure envelope and/or distribution channel before being verified on the receiver side. This process requires much time to be done. On the other side, digital documents do not need printing, and distribution process could be shortened using email and other digital channel. Digital signature would be able to replace manual signature with similar accuracy but shorter time.

3) *Streamline processes* [5,6]

Digital document and digital signature utilization makes many process become more efficient. All storing, signing, and distribution process are done using computerized system without any printing or manual distribution needed. This makes any process become smoother and more efficient.

4) *Comfortable and easy to use* [5,8]

Using digital document and digital signature, many processes become more simple. This helps not only educational staffs, but also students and student candidates. Students these days are mostly familiar with technology, so using digital signed document would be beneficial and easy for them.

5) *Increase security* [8]

Digital signature is different from digitized signature or scanned signature. Digital signature uses cryptographic algorithm to sign digital documents. This cryptographic algorithm makes digital signature is difficult to be duplicated. It could also detect if a document has been tampered or not easily. Thus, it is clear enough that using digital signature in digital document brings document security to the next level.

6) *Paperless* [6,8]

With digital signature, there is no need to print documents and sign it manually. This could reduce paper usage which is a very wise decision for the sake of mother nature.

IV. Conclusion

Digital signature could reduce time and costs in education-related and administration processes which makes them more efficient. This approach also has great security which could protect mostly integrity, authenticity, and non-repudiation (also confidentiality with some techniques) of a document. Thus, we could conclude that digital signature could be very beneficial for many sectors, including education sector.

ACKNOWLEDGMENT

First and foremost, praises and thanks to God, for His blessings and love, so I could finish this paper. I also would thank like to acknowledge my lecturer Dr. Ir. Rinaldi Munir, MT. that has been taught me about cryptography for a whole semester, especially about digital signature. I believe that this knowledge would be very beneficial not only for writing this paper but for my software/security engineer career in general.

I would also thank all my colleagues, students of batch 2016 Informatics Major in Bandung Institute of Technology, for all the support. And finally, I would express my gratitude to my family, for their support and endless love towards me that always brighten up my days.

REFERENCES

[1] A. J. Menezes, P. C. Van Oorschot and S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996.

[2] R. Munir, "Tanda Tangan Digital," Teknik Informatika STEI - ITB, Bandung.

[3] Merriam-Webster, "cryptography," Merriam-Webster, [Online]. Available: https://www.merriam-webster.com/dictionary/cryptography. [Accessed 6 May 2020].

[4] Cambridge Dictionary, "education," [Online]. Available: https://dictionary.cambridge.org/dictionary/english/education. [Accessed 07 05 2020].

[5] E-Lock, "Digital Signature for Education Sector," incVersity Limited, 2018. [Online]. Available: https://www.elock.com/Digital-signature-for-education-sector.php. [Accessed 8 May 2020].

[6] Secured Signing, "Secured Signing for Education," Secured Signing Limited, [Online]. Available: https://www.securedsigning.com/solutions/for-education. [Accessed 8 May 2020].

[7] D. Girish, "4 Ways Schools Can Benefit from Electronic Signatures," SignEasy, [Online]. Available: https://signeasy.com/blog/productivity/e-signatures-benefit-schools/. [Accessed 8 May 2020].

[8] Evolis, "Digital Signature," Evolis, [Online]. Available: https://www.evolis.com/markets/education-card-printing/digital-signature-printing. [Accessed 8 May 2020].

[9] J. O. Akpeninor, Modern Concepts of Security, Bloomington, IN: AuthorHouse, 2013, p. 135.

[10] J. Andress, The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice, S. Winterfield, Ed., Waltham: Syngress, 2014, p. 240.

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.

Surakarta, 8 Mei 2020

Ranindya Paramitha
13516006