I.J. Information Engineering and Electronic Business, 2017, 4, 1-6
Published Online July 2017 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijieeb.2017.04.01

The Implementation of Pretty Good Privacy in eGovernment Applications (Case Study on the Official Scripts Electronic Applications in Bantul)

Didit Suprihanto
Department of Electrical Engineering Universitas Mulawarman, Kalimantan Timur, Indonesia, 75123
Email: didit.suprihanto@ft.unmul.ac.id

Tri Kuntoro Priyambodo
Department of Computer Sciences & Electronics, Universitas Gadjah Mada, Yogyakarta, Indonesia, 55281
Corresponding Author
Email: mastri@ugm.ac.id

Abstract—eGovernment application has evolved from simply appearing as a website providing news and information, to the application that provides various services through online transactions. Provision of online transactions require the effectively and safely service, so the users can make sure that the entry data is secure and will not be used by other parties which are not authorized. Security is also necessary for the service provider side of online transactions, it is necessary to keep the system, and the data transactions sent through the communications media and the data stored in the database are secured. If the security guarantee is unavailable, the users will gradually lose their confidence to use the service through online transactions by using eGovernment application, and on the other hand the service provider will face the impact of the lost or corrupt data, and unauthorized access to the data which should be only accessed by involved parties based on the appropriate authority. This paper reveals the proposed strategy of Pretty Good Privacy implementation in protecting the security data messages of the Official Scripts Electronic Applications in a Local Government Regency. The proposed strategy is done by modifying on four process document letters' management, such as an electronic form of incoming mail, print or hardcopy incoming letters, disposition letter, and outgoing mail.

Index Terms—Official Electronic Papers Applications, eGovernment, PGP, Document Security, Online Transactions, Security Data.

I. Introduction

The number of online services provided by Government and private sectors is increasing. On the same pattern various countries have their own portals to provide basic services to the citizens and other people of the world [1]. The United Nations' global survey reports some ICT indicators that point to the measure of how far a nation has gone in the implementation of e-governance such as: 1.E-readiness, 2.Web measure index, 3. Telecommunications infrastructure index, 4. Human capital index, 5. E-participation index[2]

Information security is a major factor in the service of eGovernment. The using of the host to host in previous services of eGovernment is considered as lacking in security. Therefore, it needs more security to serve clients more efficiently and to obtain reliable data provided from the host [3]. There are multiple numbers of security systems are available to protect your computer/resources. Among them, password based systems are the most commonly used system due to its simplicity, applicability and cost effectiveness [4]

eGovernment application has been developed from a common website providing information and news merely into applications that provide various services for online transactions as demanded by the needs of users. On the one hand, the provision of these services will allow citizens to access and perform various activities easily. In a previous way, the citizen had to come directly to the office where the services are located, but now, it can be done from any place and any time.

Meanwhile, on the other hand, the provision of online transaction requires a secure service, both in technical and non-technical aspect, to make the users (citizens) sure and keep using the service continuously. Security related to technical services currently has a lot of concepts and tools developed, while the non-technical aspects are related to the security of the process, law factor, and security strategy to be applied [5]. This is proved with the statement that the rapidly increasing of eGovernment services users since it was introduced, it will require higher security system on eGovernment in order to make the users feel secure [6]. Technically, the security of online transaction services in the o-Government is

categorized into three levels, such as 1) The layer security application, 2) Network layer security, and 3) Data security [6]. Security at the layer level application, include 1) Authentication, 2) Data integrity, 3) Trust, 4) User Anonymity, and 5) Security Dependencies [7]. Other security features may also be required at lower layers level in the TCP/IP suite [7][8].

Security at the level of the network layer can be done by using cryptographic method and protocols that have provided security features for communication on the Internet. Security at this level include: SSL and TLS for web traffic, PGP for email, IPsec for network layer security, MIME to expand the capacity of e-mail, S / MIME to enhance security in MIME data, Message Authentication Code to encrypt a message and Firewalls for control of access between networks, Circuit-level gateways, and Application-level gateways [8][9][10].

The data security is necessary because in principle the data is confidential, and the data need to be protected from the possibility of losing data, unauthorized access (even if just seen by others without authorization). In this case, the data security is aimed to protect the database from the destructive forces and the unwanted actions of unauthorized users [11][12]. The security risks of eGovernment applications are categorized into five terms, such as 1*) information intercepting, 2) information tampering, 3) services denying, 4) systems resources stealing, and 5) information faking* [9].

An example of the proposed strategy for security and trust in eGovernment application had delivered by [13], in which the proposed strategy involved five components, such as *1) standard, 2) security policy, 30 trusted computing, 4) defense-in-depth strategy, and 5) human factor*. A proposed concept to maintain the authenticity and integrity of digital forensic evidence in the environment that is safe and reliable also had been presented by [14], in which a strategy can be applied by involving five components, such as *1) standard and forensics policy, 2) security policy, models, and trusted management system, 3) trusted computing, 4) secure channel of communication, and 5) human factor*. The following section focus how the proposed implementation strategy of PGP protects the security of data messages in the Official Scripts Electronic Applications in a Local Government Regency.

II. Telematics Data Processing Office (TDPO) in Bantul

Telematics Data Processing Office (TDPO) Bantul is one of Regional Technical Organization in Bantul regency under government environmental [15]. TDPO is a supporting element of the local government implementation headed by a chief office that is under responsible to the regent through the local secretary. TDPO has the tasks in developing and implementing a regional policy of Communication and Information. In performing the duties, TDPO of Bantul Regency is functioned to accomplish 1) the formulation of technical policy in information technology, 2) the implementation of government affairs and public service information technology, 3) providing guidance and control of information technology, 4) implementing office's administration; and 5) the implementation of other tasks given by the Regent in accordance with its duties and functions [16].

TDPO Bantul provides service for RWU (Regional Work Unit) and Public, include: 1) E-mail Officer; 2) Public Service, such as a) Enterprise Promotion for SME (small medium enterprise) and Tourism Object in Bantul, b) Free Wi-Fi / Hotspot, and c) Open Source Software; 3) RWU Service / Government Agencies (including: a) Open Source Software installation, b) RWU's official E-mail and chief of RWU, c) Sharing Application Document, d) Application Engineering Data, e) Training related to optimization of the use of information technology devices, f) Back up important data on education in the Data Center of Bantul Regency, and g) Training room and ICT training instructors; 4) E-mail for Official (Regent and the Regional Secretary); and 5) SMS Center Bantul regent.

In performing the duties and functions, TDPO Bantul is guided by local regulations, including: 1) Perda Kabupaten Bantul No. 17 Tahun 2007 ; 2) Peraturan Bupati Bantul No. 91 Tahun 2007 ; 3) Peraturan Bupati Bantul No. 76 Tahun 2011; 4) Peraturan Bupati Bantul No. 72 Tahun 2012 ; 5) Instruksi Bupati Bantul No. 03 Tahun 2011 ; and 6) Surat Edaran Sekretaris Daerah Kabupaten Bantul No. 555/4864 Tahun 2011. While the national regulations that guide TDPO Bantul, include: 1) Instruksi Presiden RI No. 03 Tahun 2003 ; 2) Peraturan Menteri Komunikasi dan Informatika RI No. 5 Tahun 2015 ; and 3) Surat Edaran Menteri Pemberdayaan Aparatur Negara RI No. SE/01/M.PAN/3/2009.

III. The Official Scripts Electronics (OSE)

The Official Scripts Electronics (OSE) is the official script management electronically by utilizing information and communication technology to give speed and ease in the decision - making process. OSE application is a management system of the script which was made by utilizing legal information and communication technology. OSE management refers to 1) Peraturan Bupati Bantul Nomor 62 Tahun 2010; 2) Peraturan Bupati Bantul Nomor 51 Tahun 2012; 3) Keputusan Bupati Bantul Nomor 342 Tahun 2003 [17]. OSE application was developed as an effort to reform the bureaucracy and to actualize good governance by replacing the manually mailing system into the computerized system for the management of documents and letters in local government offices. Application Development of OSE was developed by concerning to various laws and regulations used in the Republic of Indonesia, by providing most of the functions of office electronics which include 1) applications and web-based systems, 2) presenting information easily and appropriately, 3) electronic mail, 4) electronic folder, 5) the flow of official letter automatically in an intranet environment, 6) electronic daily agenda, 7) recording the

flow of the script automatically, and 8) the electronic documents' management.

Application Development of OSE is based on some considerations such as 1) support the policy of electronic office to the eGovernment, 2) efficiency and effectiveness of the work, 3) the efficient use of paper (paperless), 4) the savings and the ease of duplication, 5) saving storage, 6) saving the time of document searching, 7) minimize the risk of losing documents, 8) the ease of handling Official Papers documents, and 9) ease of tracking the place and status of Official Papers documents. The scope of documents that are managed in OSE application is the entire of incoming and outgoing mail which include 1) Circular Letter, 2) Common Letter, 3) Warrant, 4) Permit Letter, 5) Invitation Letter, 6) Summons, and 7) Announcement.

The architectural application of OSE that is currently running is shown in Fig. 1, while the flow document of OSE application is shown in Fig. 2.

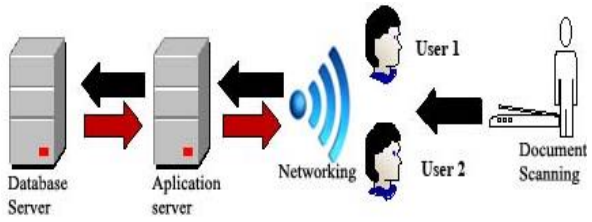

Fig.1. Architecture OSE (Source: Peraturan Bupati Bantul No. 72 Tahun 2012)

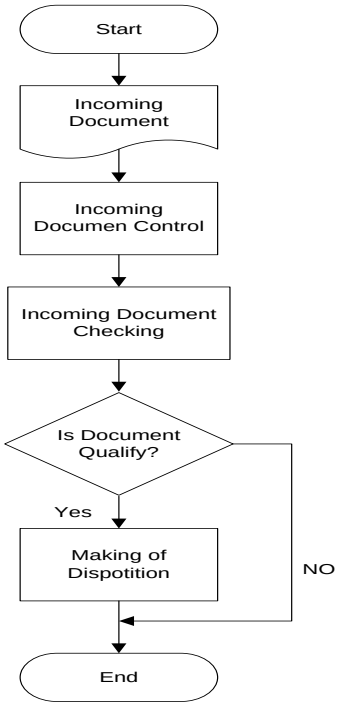

Fig.2. Flow Documents in OSE Application (Source: Peraturan Bupati Bantul No. 72 Tahun 2012)

IV. Pretty Good Privacy (PGP)

PGP (*Pretty Good Privacy)* is a multipurpose application to protect files by encrypting and/or providing a digital signature. PGP can be used by companies or individuals. Using PGP, the company or individual can exchange messages via email and/or files by providing confidentiality protection in the form of encryption and digital signature authentication form. PGP is developed based on strong cryptography algorithms such as IDEA, RSA, or SHA-1. The free version/non-paid (for personal/non-commercial) of PGP has been available since 1991, while the international version has been available for free/non-paid [18]. PGP is a hybrid cryptography system which combines the features of conventional cryptography and public key cryptography. Email encryption using PGP apply encryption algorithm asymmetric key with pair public-private key where the sender uses the public key of the receiver to encrypt secret key in the algorithm symmetry code, and finally the key will be used to encrypt original text [19].

The implementation of PGP by the company is generally based on considerations on five aspects, such as 1) *de facto* standard on the Internet, 2) integrated easily in most of all applications, file can be signed and/or encrypted, as well as in the text, 3) proven safe, 4) in most cases, the users can maintain strong control of its private key, in order to increase the users' trust, and 5) can be used either in a corporate network or for correspondence to the internet or from the internet [20]. While the applying of PGP in messaging services are covering five aspects: 1) authentication, 2) confidentiality, 3) compression, 4) e-mail compatibility, and 5) segmentation and reassembly [19].

V. PGP Implementation Strategies in OSE Application

Based on the brief description of OSE application in Bantul regency, the following description will review the proposed draft implementation strategy for the PGP application documents security in OSE Applications. Broadly speaking, the proposed strategy includes:

A. The implementation of PGP in inbox/incoming mail electronic form (Model 1)

Inbox is a received letter/mail from outside parties intended to RWU (regional work unit)/work unit/elected officials. OSE system will perform agenda of managing incoming mail automatically, so all the data stored in the host computer. PGP workflow application of incoming mail is shown in Fig. 3.

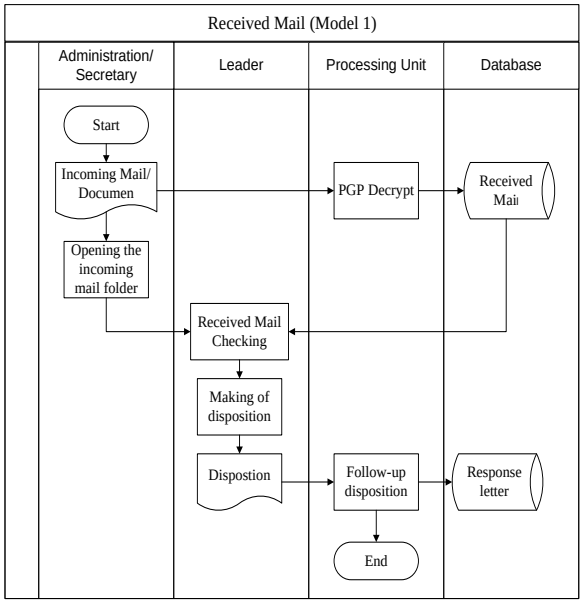

Fig.3. The implementation of PGP in the Inbox (received mail) Electronics Form of OSE Application

B. The implementation of PGP in inbox (received letter) in the form of print/hardcopy (Model 2)

Incoming mail in hardcopy form must be undertaken through scanning (scanning) documents. Scanning is done to facilitate the archiving in the host computer. Workflow inbox print form is shown in Fig. 4.

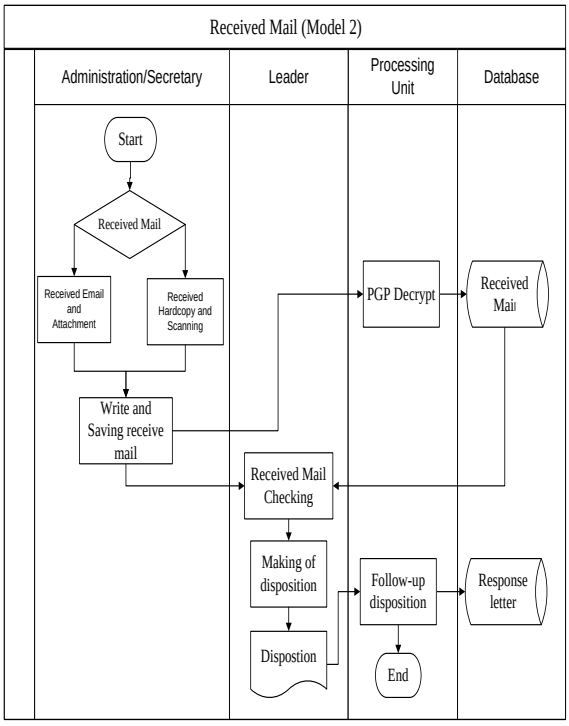

Fig.4. The implementation of PGP in the Inbox Form Print/Hardcopy in OSE Applications

C. Applying PGP on Disposition Letter

Disposition is a tool for two-way communication from superiors to subordinates and vice versa, in responding the incoming mail. The workflow of the disposition letter is shown in Fig. 5.

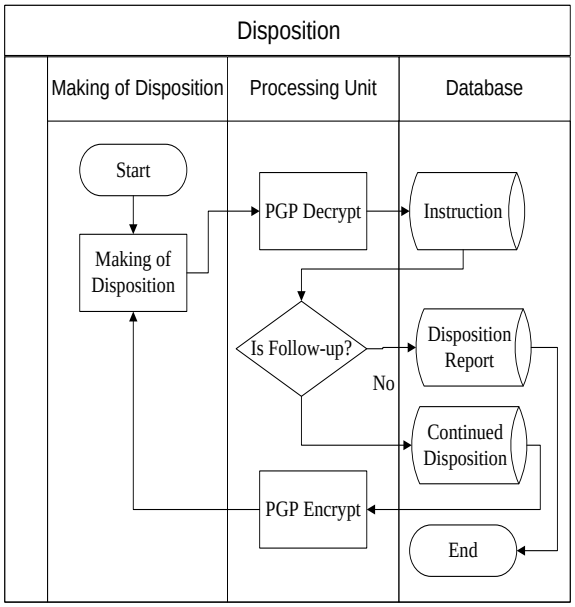

Fig.5. Application of PGP on Disposition Mail in OSE Application

D. The implementation of PGP in the outgoing mail

Outgoing mail/letter is a letter which is sent to outside parties made by RWU/unit/elected officials. OSE system will provide facilities for the preparation of a draft letter by Bantul Regent Regulation governing the Code of Official Scripts of Bantul Regency. Numbering outgoing mail and storage is done automatically. Dispatching is done electronically or in hardcopy form, as shown in Fig. 6.

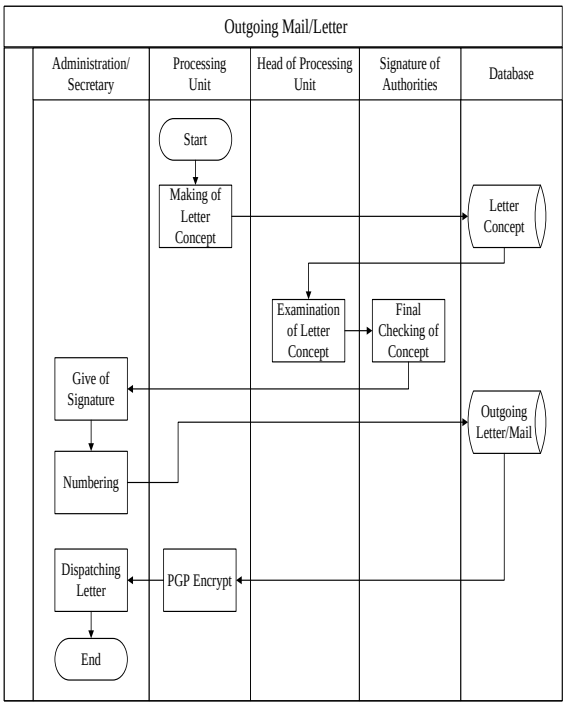

Fig.6. The implementation of PGP in the Outgoing Mail of OSE Application

VI. Results and Discussion

To implement the proposed strategy document security, it can be done by using PGP application by OSE application toward the Regent regulation of Bantul Number. 72, 2012, it can be done through the following mechanisms:

A. OSE Application Security

OSE application provides user authentication features that use the system applications access. The authentication mechanism is done by using username and password checking, so that the users who are successfully logged into the system can access the application in accordance with the authority that has been determined for each user. Authentication feature is also equipped with a safety system that ensures that the data is entered by the user and not by another system/virus, for example by applying the authentication using an image, a special article (capture), or security question. Authentication access to the application system must be guaranteed that:

1. Applications can only be accessed by authenticated users.
2. Users can only access the menu that belongs to their authority.
3. The same username cannot be used in parallel at the same time.

B. User Event Logging

OSE application is equipped with features to record every user activity associated with the system. The activity log is used to conduct examining of all activities performed by the user on the OSE application.

C. Implementation of PGP applications in TNDE application.

Implementing the PGP application in TNDE application that consists of five components, they are:

1. *Authentication*: in this component, there are two services provided. The first service identifies the authenticity of a message or a script and guarantees its authenticity. The second service, testing someone's identity or if the user will enter a system.
2. *Confidentiality*: provide confidentiality of the messages which are going to be sent and save the messages or data by using the encryption techniques. PGP encryption techniques on a plain text (e-mail) to randomized text, to make sure or giving guarantee that the message was sent and until the recipient receives and opens the message, it is still secure and will not be amended (message integrity)
3. *Compression*: the default PGP application has applied compression of text message or script that will be sent. The compression process is done before passing to the encryption process. It is intended to provide space saving advantages of sending e-mail and file storage.
4. *E-mail compatibility*: this component is used to facilitate the use of e-mail application easily, so that the encrypted message can be encrypted into a string of ASCII format.
5. *Segmentation*: restrictions on the size of the message that will be sent is done by segmentation component. In the PGP application, segmentation process and rearrangements occur in large messages to be sent.

The proposed of PGP implementation strategy for documents security in OSE application can be applied to the requirements that consist of two aspects, such as: 1) infrastructure requirements, and 2) the requirements of the superstructure. The strategy in applying PGP of documents security in OSE application provide benefits, such as: 1. Security, the applying of PGP deployments in OSE application will provide security documents communicated; 2) Effectiveness, application deployment of PGP in OSE applications will provide the effectiveness of the process of conducting the official scripts in local government as efforts to achieve good governance, this can happen because the service is effective and safe, so that the user s are sure that the data entry is secure and will not be used by other parties that are not authorized; 3) The efficiency, applying deployment of PGP in OSE applications will provide cost efficiency, because it is not charged/paid (low cost); and 4) The ease of PGP application is a tool that has been embedded (plug-in) in some web browsers and used by all e-mail programs, so it is easy and can be used flexibly.

VII. Conclusion

PGP as an application message security can be applied in OSE application by implementing five major components of PGP, including: authentication, confidentiality, compression, e-mail compatibility, segmentation. The strategy proposal is done by modifying the four letters document management process, such as: incoming mail electronic form, the incoming letter print or hardcopy form, disposition letter, and also outgoing mail. Implementation of the PGP application will provide benefits and advantages on four aspects: safety, effectiveness, efficiency, and ease of implementation of the official scripts in local government as efforts to achieve good governance.

Acknowledgments

Thank you to the Department of Computer Science and Electronics, Gadjah Mada University for the support of research facilities in the completion of doctoral degree studies.

REFERENCES

[1] Chander, S., and Kush, A., 2012, Web Portal Analysis of Asian Region Countries, *I.J. Information Engineering and Electronic Business*,Vol. 4, 25-32
[2] A. B Adeyemo, e-Government Implementation in Nigeria: An Assessment of Nigeria's Global e-Gov Ranking, Journal of Internet and Information System, Vol. 2 (1), pp. 11-19, 2011
[3] Priyambodo, T.K., and Suprihanto, D. 2016. Information Security On Egovernment As Information-Centric Networks. International Journal Of Computer Engineering In Research Trends. Volume 3, Issue 06, July-2016, Pp.360-365.
[4] Singh, P.I., and Thakur, G.S.M., 2012, Enhanced Password Based Security System Based on User Behavior using Neural Networks, I.J. Information Engineering and Electronic Business, Vol. 2, 29-35
[5] Wimmer, M., and Bredow, B. Von. 2002. A Holistic Approach For Providing Security Solutions In E-Government. Pp.1–10.
[6] Upadhyaya, P., Shakya, S., and Pokharel, M. 2012. Information Security Framework for E-Government Implementation in Nepal. 3(7), pp.1074–1078.
[7] Mehta, M., Singh, S., and Lee, Y. 2007. Security in E-Services and Applications. Network Security: Current Status and Future Directions, pp.157–177.
[8] Rhee, M.Y. 2003. Internet Security : Cryptographic Principles, Algorithms and Protocols. The Atrium, Southern Gate, Chichester, West Sussex PO19 8SQ, England. John Wiley & Sons Ltd.
[9] Zhou, Z., and Hu, C. 2008. Study on the E-government Security Risk Management. 8(5), pp.208–213.
[10] Zhang, W. 2010. E-government Information Security: Challenges and Recommendations Wei. In 2010 International Conference on Computer Application and System Modeling (ICCASM 2010).
[11] Office of the Government Chief Information Officer Ministry of Labour Citizens' Services and Open Government. 2011. Information security policy British Colombia, version 1.0.
[12] Wimmer, M., and Bredow, B. Von. 2001. E-Government : Aspects of Security on Different Layers. pp.350–355.
[13] Priyambodo, T.K., and Prayudi, Y. 2016. A Proposed Strategy for Secure and Trusted Environment in e-Government. pp.449–459.
[14] Prayudi, Y., and Priyambodo, T.K. 2015. Secure and Trusted Environment as a Strategy to Maintain the Integrity and Authenticity of Digital Evidence. 9(6), pp.299–314.
[15] Peraturan daerah kabupaten bantul Nomor 17, 2007. Pembentukan Organisasi Lembaga Teknis Daerah di Lingkungan Pemerintah Kabupaten Bantul. , pp.1–16.
[16] Peraturan Bupati Bantul Nomor 91, 2007. Rincian Tugas dan Tata Kerja Kantor Pengolahan Data Telematika Kabupaten Bantul. , pp.1–10.
[17] Peraturan Bupati Bantul Nomor 72, 2012. Pedoman Tata Naskah Dinas Elektronik di Lingkungan Pemerintah Kabupaten Bantul. , pp.1–20.
[18] Zimmermann, P. 1997. PGP-Pretty Good Privacy.
[19] Ariyus, D. 2008. Pengantar Ilmu Kriptografi : Teori, Analisis dan Implementasi. Penerbti Andi. Yogyakarta.
[20] SANS Institute. 2003. A corporate implementation of PGP. Global Information Assurance Certification Paper, (Security 401).

Authors' Profiles

Didit Suprihanto, Currently he is a PhD Student at Department of Computer Science and Electronics Gadjah Mada University and lecturer at Department of Electrical Engineering, Mulawarman University, Samarinda, Indonesia. His research interests include computer networks security and eGovernment related issues, security assesment.

Tri K. Priyambodo Since 2008, he has been an Associate Professor with the Department of Computers and Electronics, UniversitasGadjahMada, Indonesia. From 2010 to 2013 he was responsible for the development of Indonesia Inter-University Student Satellite Project as National Project Leader. He is the author of five books, more than 35 articles. His research interests include intelligent control systems, autonomous unmanned systems, satellite and aerospace electronics, computer networks security and eGovernment related issues.

How to cite this paper: Didit Suprihanto, Tri Kuntoro Priyambodo,"The Implementation of Pretty Good Privacy in eGovernment Applications (Case Study on the Official Scripts Electronic Applications in Bantul)", International Journal of Information Engineering and Electronic Business(IJIEEB), Vol.9, No.4, pp.1-6, 2017. DOI: 10.5815/ijieeb.2017.04.01

