Society, 8 (2), 628-639, 2020
P-ISSN: 2338-6932 | E-ISSN: 2597-4874
https://society.fisip.ubb.ac.id

# Digital Signature Implementation as a New Smart Governance Model

**Nursani Budiarti [1,*] Yahya Pandega Putra [1,] and Achmad Nurmandi [2]**
[1] Master of Government Science, Jusuf Kalla School of Government,
Universitas Muhammadiyah Yogyakarta, 55183, Yogyakarta, Indonesia
[2] Department of Political Islam - Political Science, Jusuf Kalla School of Government,
Universitas Muhammadiyah Yogyakarta, 55183, Yogyakarta, Indonesia
* Corresponding Author: nursani.budiarti@gmail.com

**ARTICLE INFO**

***Publication Info:***
*Literature Review*

***How to cite:***
*Budiarti, N., Putra, Y. P., & Nurmandi, A. (2020). Digital Signature Implementation as a New Smart Governance Model. Society, 8(2), 628-639.*

***DOI:*** *10.33019/society.v8i2.222*



**Received:** August 22, 2020;
**Accepted:** November 9, 2020;
**Published:** December 30, 2020;

**ABSTRACT**

*With the times, nothing is impossible with internet technology. One of the advantages of the internet is that it allows for developing it to support creativity and openness to the public, especially ICT-based governance or smart governance, by implementing digital signature, both in public services implementation and in correspondence and other documents. Most of the previous digital signature studies were limited to technical research on digital signature' patterns and design. This study aims to describe digital signature implementation as a new smart governance model. This study uses a qualitative research method and data sources consisting of reference data from various previous studies and data sourced from national online media news. Based on the analysis results using NVivo 12 Plus software, digital signature implementation is needed to anticipate cybercrime threats in effective, efficient, and accountable public services implementation as a new smart governance model.*

***Keywords:*** *Cybercrime; Cybersecurity; Digital Signature; Public Service; Smart Governance*

## 1. Introduction

The more rapid the development of technology, the more challenges will arise with it. With the advancement of technology, everyone can easily do everything faster and shorter. One of these technological developments is the internet. The majority of internet users in Indonesia use the internet daily (Darmayani, 2018). Currently, the internet is not only used as a support for work, but the internet has also become an inseparable part of human life. Hence, the influence of the internet is in every aspect of human life. Apart from being used as work support, it is also for everyone's personal needs. The internet has become the door and window to the world, a broader and more limitless world. Nothing is impossible with internet technology, starting from the simplest things, namely looking for news to communicating with relatives or friends in other parts of the world. One of the advantages of the internet is that it allows for developing it to support creativity and openness to the public. It makes the internet very flexible for further developments that encourage the emergence and development of online innovation (Septianingrum et al., 2018).

Concerning current internet usage, data reported by Google Consumer Barometer based on survey results in 2017 shows that as follows:

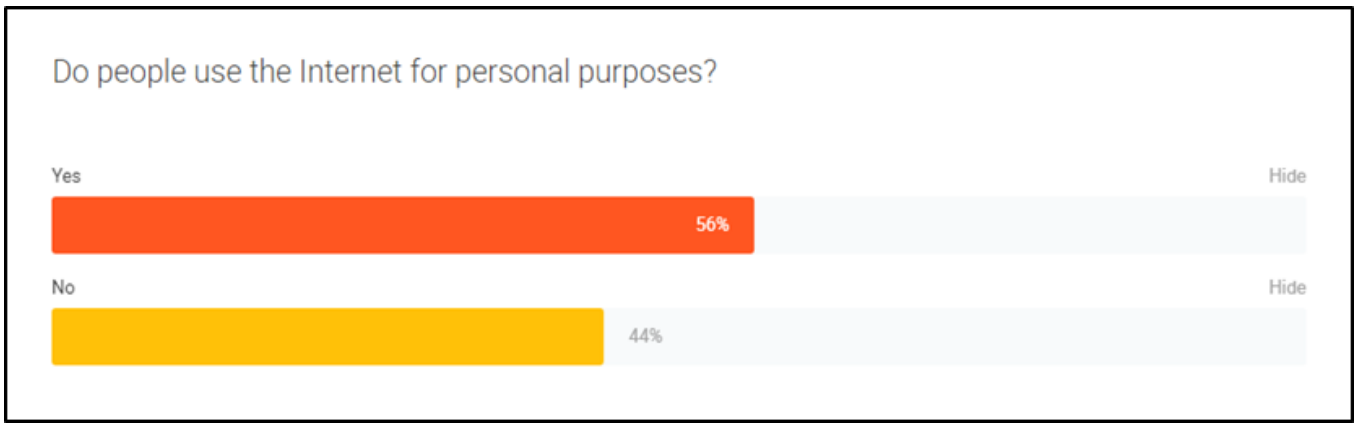


**Figure 1. Internet Use for Personal Purposes**
Source: Google Consumer Barometer (2017a)

Based on **Figure 1**, from a population of 1,000 respondents online and offline in 2017, 56% of respondents use the internet for personal purposes, and 44% use the internet, not for personal purposes.

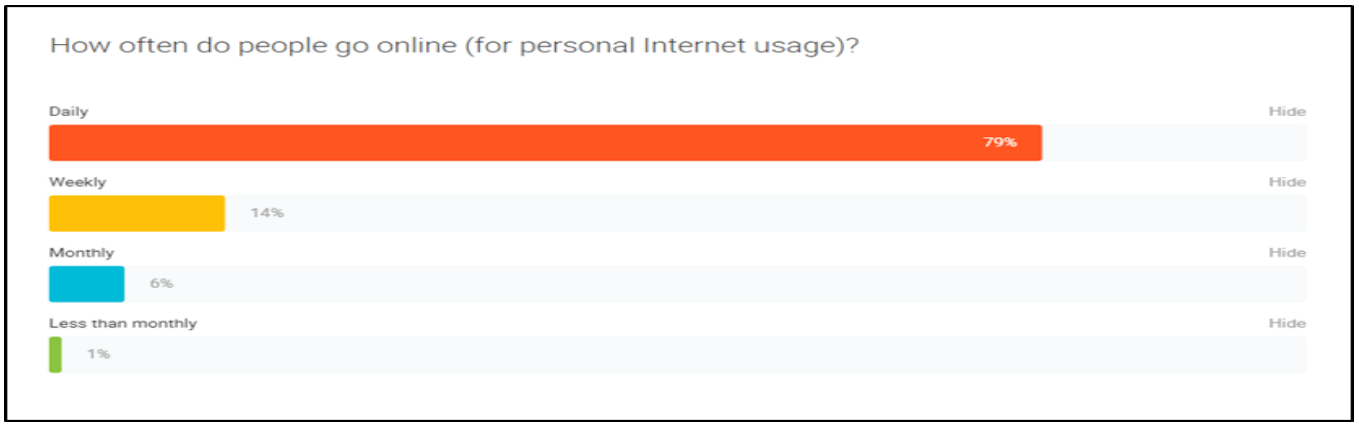


**Figure 2. Personal Internet Usage**
Source: Google Consumer Barometer (2017b)


https://doi.org/10.33019/society.v8i2.222

Based on **Figure 2**, from a population of 604 online respondents in 2017, who access via computers, Tablets, and Smartphones for personal purposes, it shows that 79% of respondents access the internet daily, 14% access the internet weekly, 6% access the internet monthly, and 1% of respondents access the internet less than monthly.

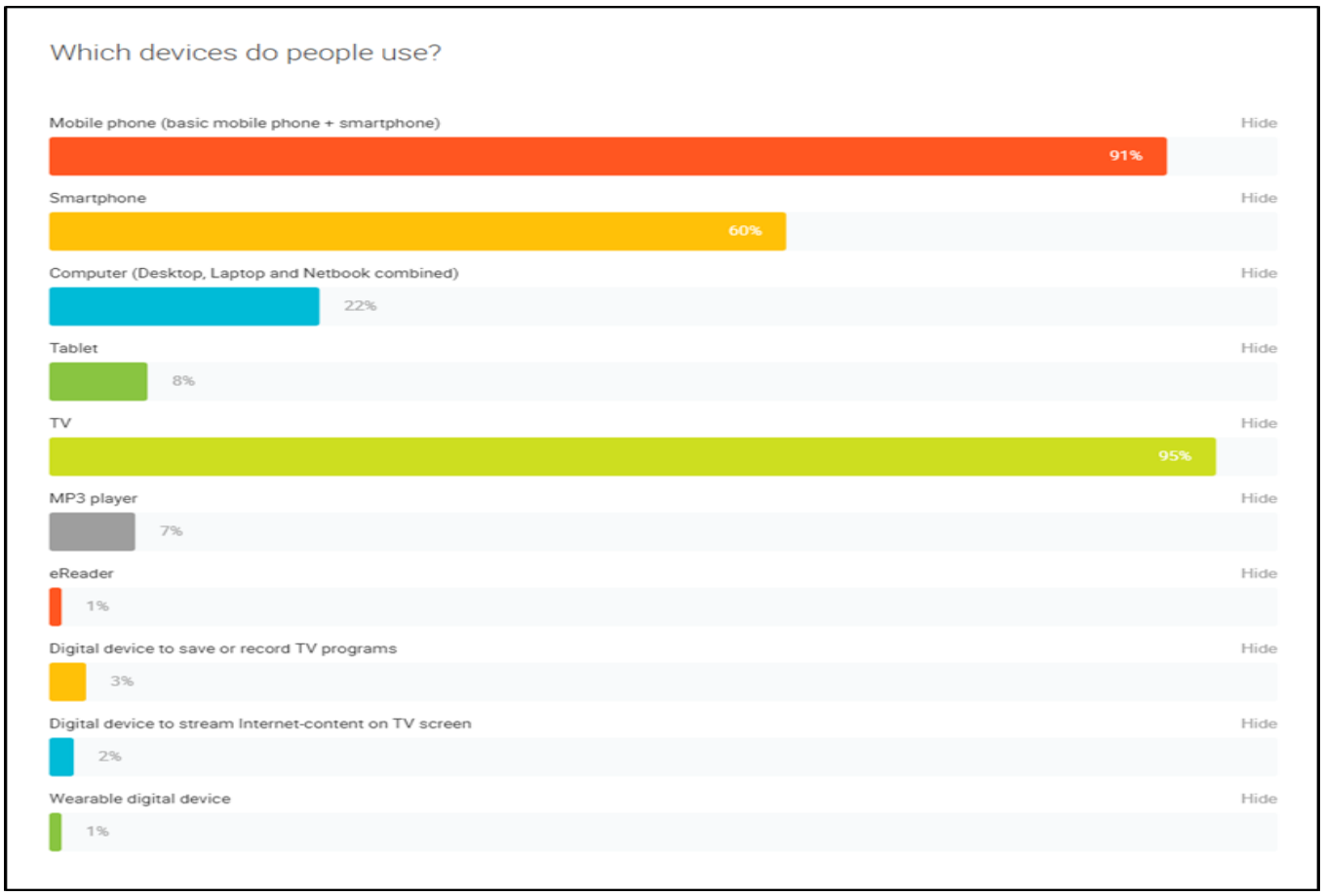


**Figure 3. Device Used**
Source: Google Consumer Barometer (2017c)

Based on **Figure 3**, from a population of 1,000 respondents online and offline in 2017, 91% of internet access via mobile phone (basic mobile phone and smartphone). Moreover, 60% use smartphone, 22% use computer (desktop, laptop, and notebook combine), 8% use tablet, 95% use television, 7% use MP3 player, 1% use eReader, 3% use digital devices to save or record TV programs, 2% digital device to stream internet-content on TV screen and 1% use wearable digital device.

All three figure above shows how the pattern of technological development, especially the internet, is increasingly massive. It forces the government to prepare cybersecurity standards. Without secure and precise cybersecurity standards, threats will continue to increase. One of the government's cybersecurity measures is implementing a digital signature on official government documents. The digital signature consists of electronic information related to other electronic information as a verification or authentication system. In Indonesia, a digital company has the authority to accept registration, verify, and issue electronic certificates and electronic signatures for Indonesian citizens and has been registered and recognized by the Ministry of Communication and Information of the Republic of Indonesia, named PrivyID.


https://doi.org/10.33019/society.v8i2.222

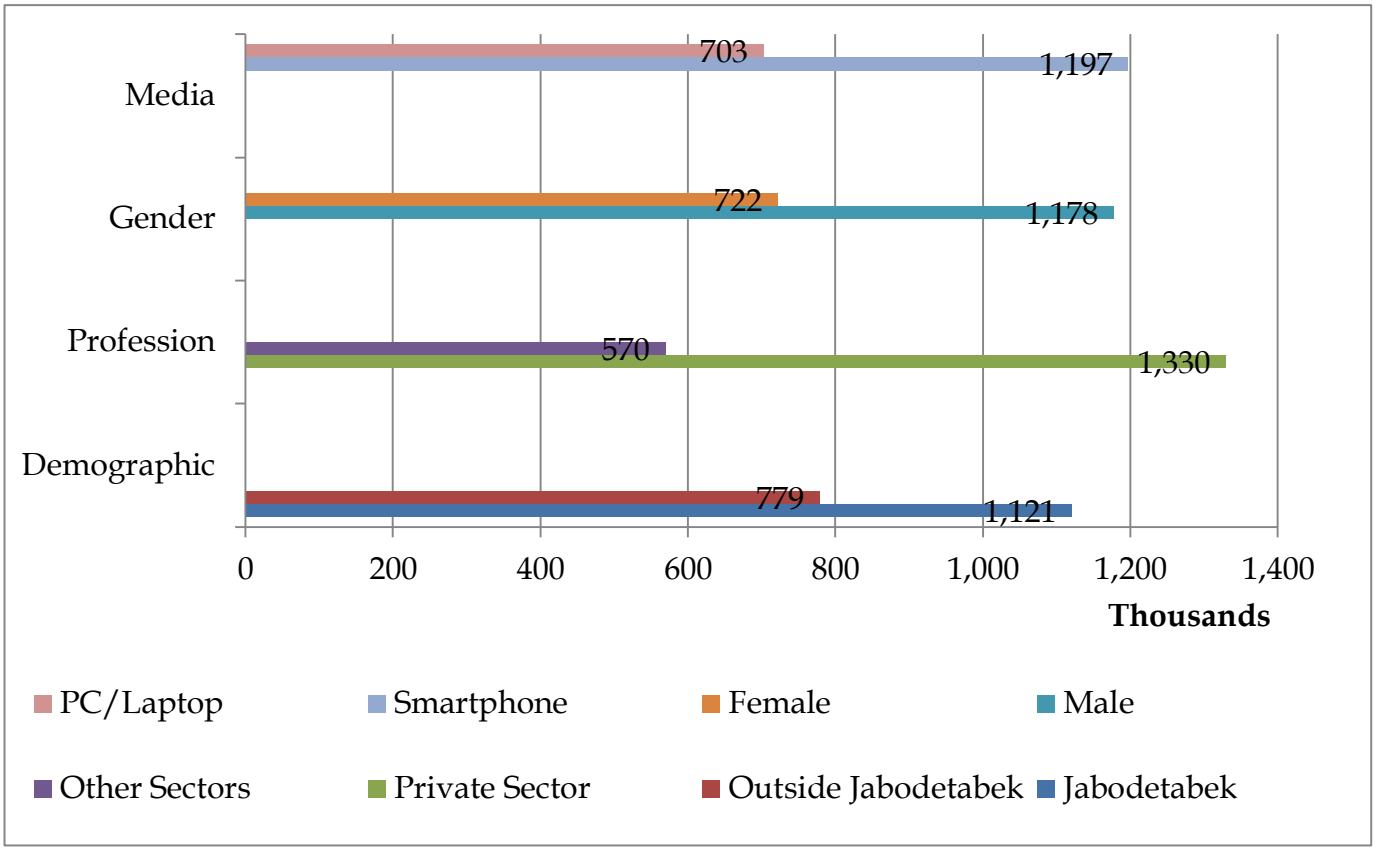


**Figure 4. PrivyID Digital Signature User in 2018**
Source: Selular.id (2018)

Based on **Figure 4**, in 2018, PrivyID digital signature users were 1.9 million. Based on demographics, 59% of digital signature users are in Jakarta-Bogor-Depok-Tangerang-Bekasi (Jabodetabek) and 41% outside Jabodetabek. If disaggregated by profession, 70% of digital signature users in 2018 were private-sector workers, and 30% were other sector workers. Meanwhile, if disaggregated by gender, 62% were male users, and 38% were female users. Based on the use of operating media, as many as 63% of users signed documents via smartphones, and some 37% used personal computers (PCs) or laptops.

## 2. Literature Review

ICT developments, which consists of the Internet of Things (IoT), the Internet of Everything (IoE), and the Internet of Nano Things (IoNT), are new approaches to integrate the internet into personal, professional, and community life (Miraz et al., 2015). Many cities or regions use this approach to implement governance, planning, and managing a city or region.

In general, to be called a large and prosperous city or area, cities worldwide have good quality and standards in various activity and public lives. Urban and regional planning is needed to improve government governance, technological innovation, public welfare, and business investment qualities to realize a Smart City. Smart City predicate obtained by developing smart infrastructure governance using ICT to find and analyze data needed by the government, public, and other stakeholders. Being a smart city also means must continue to innovate and develop in a better way.

Smart governance is the main requirement in implementing Smart City development. The government must shape the public's paradigm of a better life. Public trust in the government can be grown by showing concern and transparency in governance administration. In


https://doi.org/10.33019/society.v8i2.222

implementing government governance, a good governance concept is a primary key to its success. The concept is a paradigm, system and government governance, and development based on law principles. Smart governance aims to realize effective, efficient, and communicative governance and continuously improve the bureaucracy's performance through innovation and integrated technology adoption.

The increasingly massive technological development pattern, especially the internet, forces the government to prepare cybersecurity standards for existing internet networks, especially ICT-based governance administration. Without fast and precise cybersecurity standards, the threat will increasingly increase, called cybercrime. Cybercrime is unlawful activities in which computers or computing devices such as smartphones, tablets, Personal Digital Assistants (PDAs), and other devices that stand-alone or part of a network used as tools and or as targets for criminal activity. People with destructive and criminal mindsets often carry out cybercrime for revenge, greed, and gain experience (Pande, 2017).

The cybercrime threats types consist of 1) The theft of personal data for commercial purposes, such as theft of identity and credit card numbers; 2) Illegal access to company data used for business competition; 3) The theft of government data used to attack a specific entity; 4) Collecting intelligence data of a country for the benefit of a foreign country or specific entity; 5) Data manipulation for political or business purposes; 6) Attacks aimed at eliminating control or weakening or even paralyzing the government or a company; 7) Manipulation of internet user behavior to download Malicious Software (Malware) which aims to infiltrate and destroy systems, and 8) Direct attacks via internet network against systems that aim to cripple public services of specific public institutions (Ahmad et al., 2018).

The ICT-based governance process trimmed long bureaucracies to effectively and efficiently public service process without contradicting the prevailing laws and regulations. Bureaucracies sometimes cause delays in the public services process and government policy decision-making. In making bureaucracies' simplification, needs an effective and efficient system without reducing governance accountability by implementing digital signatures in public services and the correspondence process and other government administration documents. A digital signature consists of electronic information related to other electronic information as a system of verification or authentication. A digital signature is not a scanned signature and then embedded into a document, but rather a series of data and information embedded into a document.

A digital signature is one of the cybersecurity policies implemented in anticipating data and official document manipulation issued. Three basic digital signature processes consist of checking signatory authentication, document authentication, and digital signature verification. Its development uses several algorithms, such as Elgamal and Schnorr (Pooja & Yadav, 2018).

Digital signature implementation in governance is increasing, starting from document management in official correspondence until used in the government's licensing documents. Using a digital signature can guarantee that the document is authentic (Liyanti & Hakim, 2019) because it can authenticate the signed document and the signature owner through an algorithm (Perdana et al., 2019). There are two types of digital signatures: uncertified digital signature and certified digital signature. Types of uncertified digital signatures, for example, are scanned wet ink signatures, Barcodes, QR codes, and Biometrics. In contrast, examples of certified digital signatures are signatures using cryptography or called a digital signature.

Digital signature as a new smart governance model aims to encourage accountable smart governance further to develop cybersecurity (Febrianta et al., 2019). Besides, implementing a digital signature policy is also in line with implementing smart governance, especially in good


https://doi.org/10.33019/society.v8i2.222

government management, and creating a positive image of modern and progressive government (Kumar, 2015).

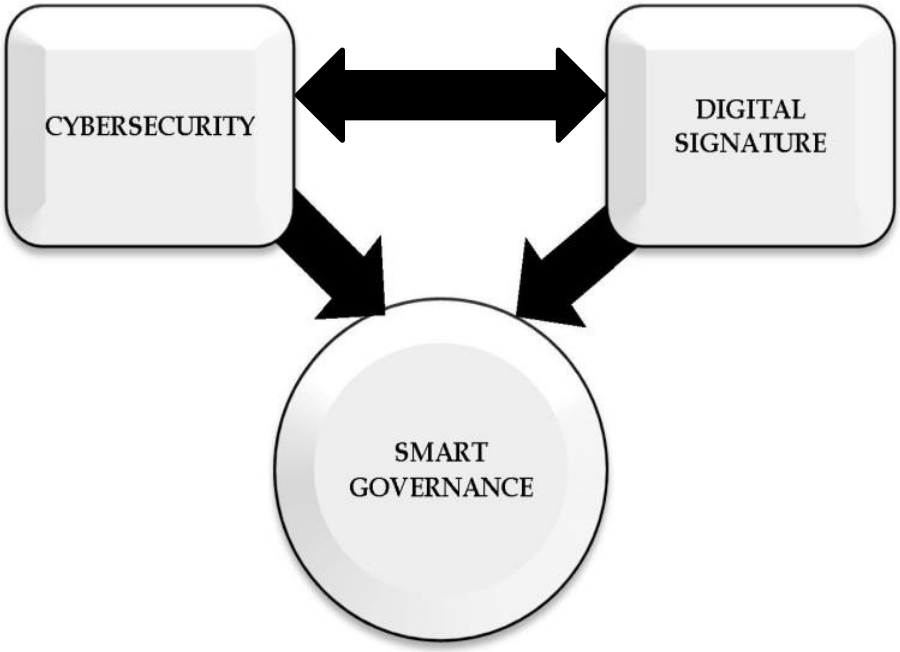


**Figure 5. Conceptual Framework**

**Figure 5** above illustrates that this study's conceptual framework from the smart governance concept emphasizes cybersecurity policies with digital signature implementation to anticipate manipulating data and official documents issued by the government to implement the governance process effectively, efficiently, and accountable.

## 3. Research Methodology

This study's conceptual framework based on smart governance implementation requires cybersecurity policies using digital signatures (**Figure 5**). This study aims to describe digital signature implementation as a new smart governance model to implement effective, efficient, and accountable public services.

This study uses a qualitative research method and data sources consisting of reference data from various previous studies and data sourced from national online media news using NVivo 12 Plus software with the NCapture feature. This feature capable of systematically extracting data from national online media with in-depth analysis. The use of national online media in this study aims to complement the literature review used as a reference. The NVivo 12 Plus software use aims to map and explore cybersecurity policies implementation using digital signatures in smart governance.

## 4. Results and Discussion

Some of the functions of implementing smart governance are 1) Policymaking and implementation of regulatory and development functions run well; 2) Quick data acquisition, storage, and retrieval; 3) Improved governance management; 4) Increasing the dissemination of rules, regulations, and government activities; 5) Improved performance in the setting function; 6) Improved performance in the social sector; and 7) Creating a positive image of a modern and progressive government (Kumar, 2015).


https://doi.org/10.33019/society.v8i2.222

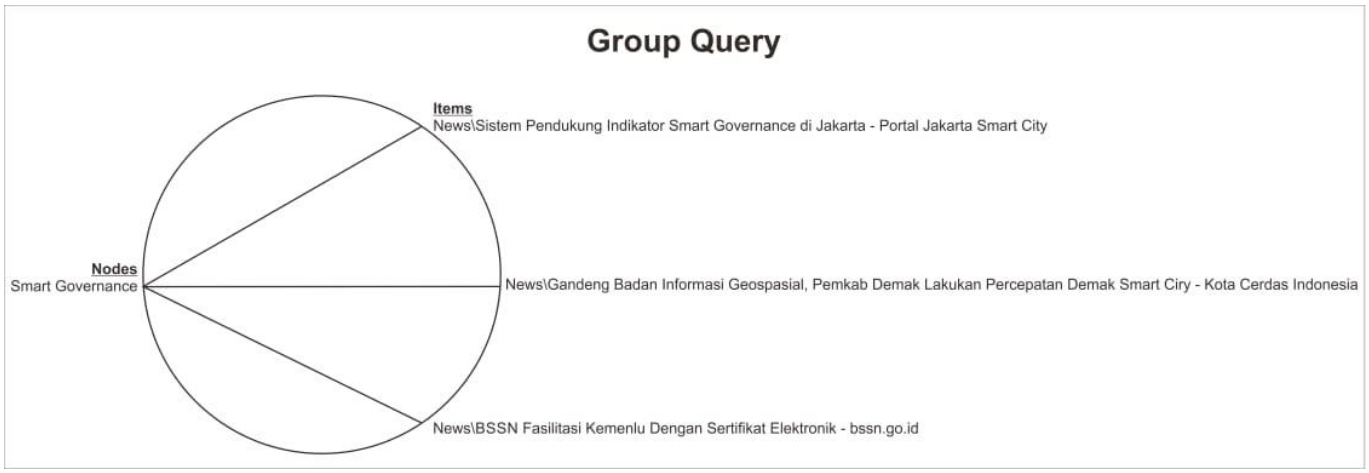


**Figure 6. Smart Governance**
Source: NVivo 12 Plus (processed data result)

**Figure 6** shows two national online media reports on smart governance, especially reports on smart cities, and national online news concerning electronic certificates. As part of a smart city, smart governance requires applying policies on electronic certificates.

The increasingly massive pattern of technological developments, especially the internet, forces the government to prepare cybersecurity standards for the existing internet network, especially in the administration of ICT-based governance. Without cybersecurity measures that are fast and precise, the threat will increasingly increase called cybercrime.

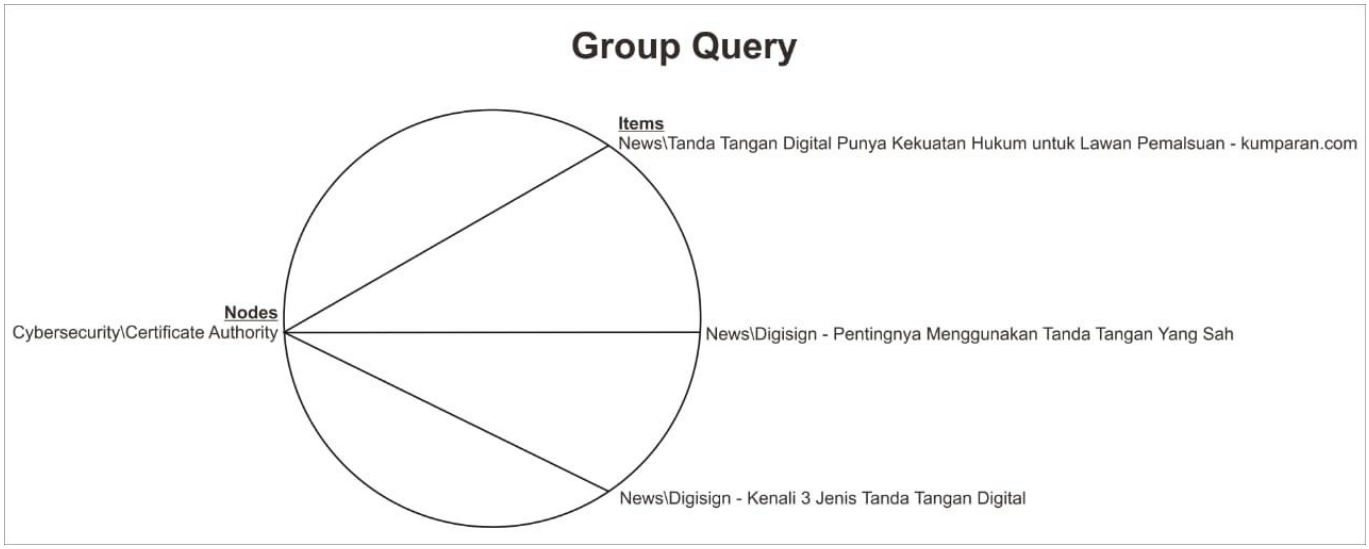


**Figure 7. Cybersecurity**
Source: NVivo 12 Plus (processed data result)

**Figure 7** shows that some national online news reports about cybersecurity policies. Cybersecurity is a policy that must be carried out by the government to anticipate the threat of cybercrime.


https://doi.org/10.33019/society.v8i2.222

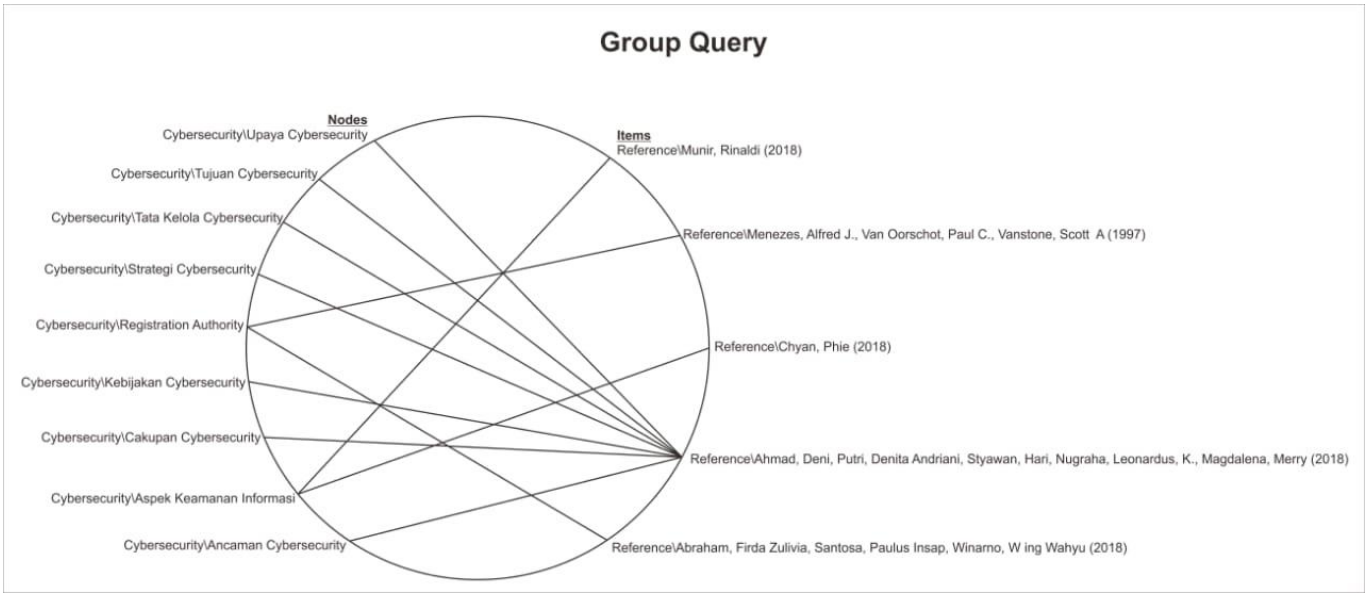


**Figure 8. Studies on Cybersecurity**
Source: NVivo 12 Plus (processed data result)

**Figure 8** shows that five studies examine cybersecurity, consisting of:

1) Rinaldi Munir conducted a study on information security aspects and stated that digital signatures are not limited to embedding in digital documents. It can also embed in the software to maintain integrity for documents and software (Munir, 2015).
2) Alfred J. Menezes, Paul C. van Oorschot, & Scott A. Vanstone, in their book entitled "Handbook of Applied Cryptography," described the registration authority. The process is one of the processes in digital signatures issuance that aim to maintain confidentiality, integrity, entity authentication, and data authentication (Menezes et al., 1997).
3) Phie Chyan conducted a study on information security aspects and stated that following ICT development advantage, there is one thing that should concern the government: information security. The information must be maintained not to be recognized by unauthorized people (Chyan, 2018).
4) Deni Ahmad, Dinita Andriani Putri, Hari Styawan, Leonardus K. Nugraha, & Merry Magdalena conducted a study on policies, governance, strategies and efforts, coverage, goals, and cybersecurity threats (Ahmad et al., 2018).
5) Firda Zulivia Abraham, Paulus Insap Santosa, & Wing Wahyu Winarno conducted a registration authority study. The registration authority is a digital signature authentication model used for electronic documents created, sent, or stored either in analog or digital types or in other types (Abraham et al., 2018).

The government must apply cybersecurity policies in the governance process to anticipate cybercrime threats in implementing smart governance.


https://doi.org/10.33019/society.v8i2.222

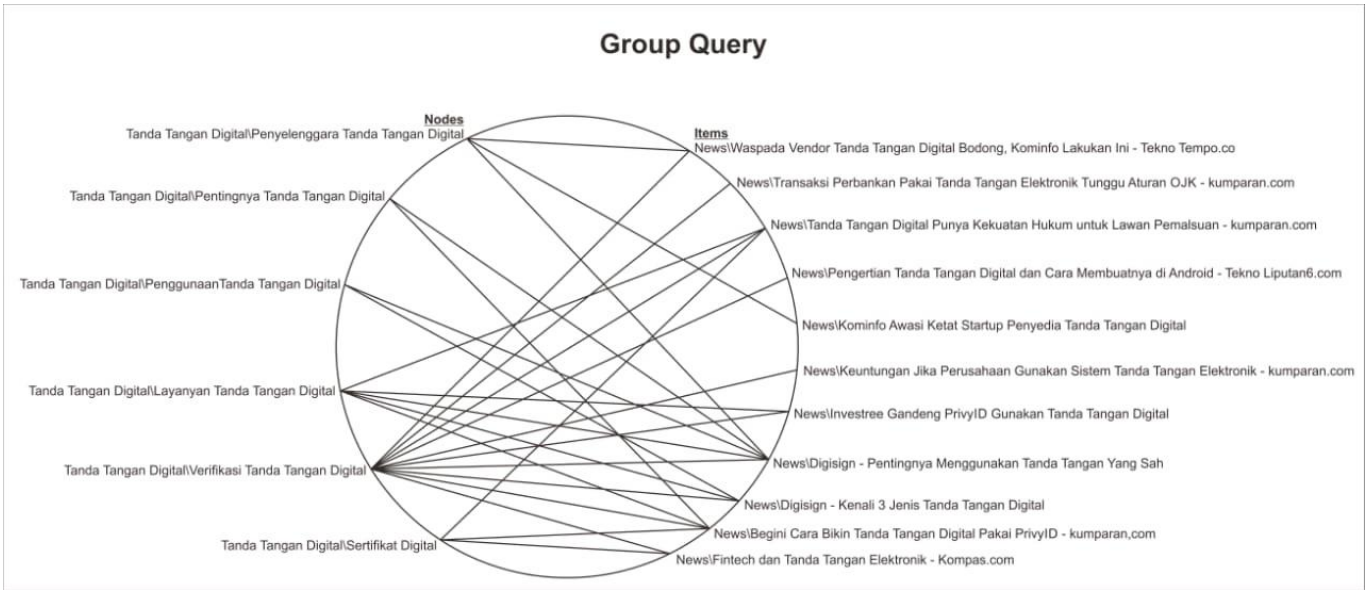


**Figure 9. Digital Signature**
Source: NVivo 12 Plus (processed data result)

**Figure 9** shows that many national online media report about the use of digital signatures. Digital signature validity processes are the most reported by ten national online media. In comparison, digital signature services rank second with the news carried out by five national online media, third place concerning digital signatures validity using digital certificates and digital signatures implementation reported by three national online media and the rest regarding the use and importance of digital signatures reported by two national online media. Digital signatures in cybersecurity policies framework in implementing smart governance are considered the right policy for many parties.

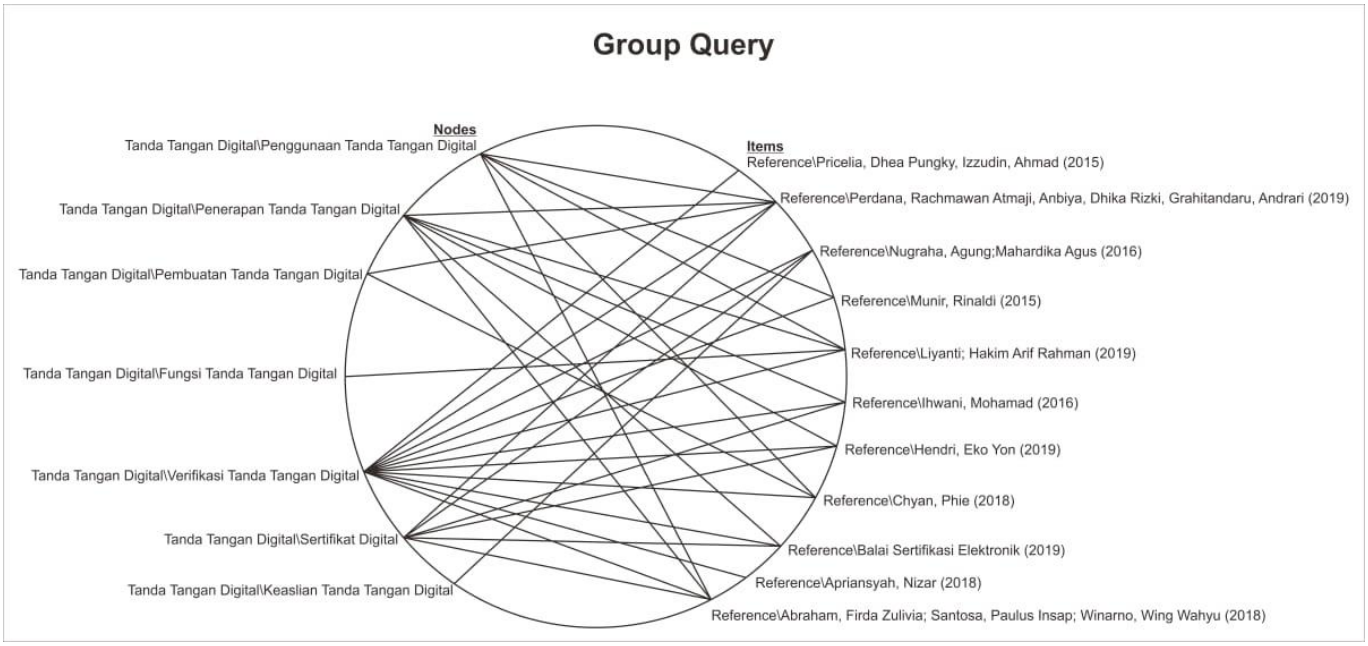


**Figure 10. Studies on Digital Signature**
Source: NVivo 12 Plus (processed data result)

**Figure 10** shows that there have been many studies examining digital signatures. The


https://doi.org/10.33019/society.v8i2.222

validity of digital signatures through the digital signature verification process is the most studied topic. In general, all studies that examine the topic of digital signature verification mostly states the security aspects of digital signatures, including the use of the Message Digest 5 (MD5) algorithm (Precilia & Izzuddin, 2015), RSA algorithm (Ihwani, 2016), digital certificates on digital signatures (Perdana et al., 2019), and others. The security factor of data protection is a priority to maintain confidentiality, integrity, entity authentication, and data origin authentication.

Using NVivo 12 Plus software, the analysis results showed that using digital signatures to anticipate cybercrime in implementing cybersecurity policies is an urgent need for the government. It is in line with the smart governance concept, which emphasizes cybersecurity policies with digital signatures implementation as anticipation of manipulating data and official documents issued by the government so that the governance process becomes effective, efficient, and accountable.

## 5. Conclusion

Digital signatures as a model of implementing cybersecurity policies in smart governance implementation are policies needed by the government in anticipating cybercrime. Analysis using NVivo 12 Plus software results, as follows: 1) Smart governance, as part of a smart city, requires applying a policy on the use of electronic certificates. 2) Cybersecurity is a policy that must be carried out by the government to anticipate cybercrime threats. 3) The use of digital signatures as a new smart governance model is considered the right policy by many parties. Based on the analysis results using NVivo 12 Plus software, a new smart governance model in digital signatures implementation is needed to anticipate cybercrime threats in implementing effective, efficient, and accountable public services.

## 6. Acknowledgment

The authors are grateful to express gratitude to those who have had the pleasure to cooperate during this study.

## 7. Declaration of Conflicting Interests

The authors have declared no potential conflicts of interest concerning the study, authorship, and/or publication of this article.

## References

Abraham, F. Z., Santosa, P. I., & Winarno, W. W. (2018). Tandatangan Digital Sebagai Solusi Teknologi Informasi dan Komunikasi (TIK) Hijau: Sebuah Kajian Literatur (Digital Signature as Green Information and Communication Technology (ICT) Solution: A Review Paper). *Masyarakat Telematika Dan Informasi: Jurnal Penelitian Teknologi Informasi dan Komunikasi*, *9*(2), 111-124. http://dx.doi.org/10.17933/mti.v9i2.120

Ahmad, D., Putri, D. A., Styawan, H., Nugraha, L. K., & Magdalena, M. (2018). *Kebijakan Cyber Security Dalam Perspektif Multi Stakeholder*. Jakarta, Indonesia: Kementerian Komunikasi dan Informatika Republik Indonesia.

Chyan, P. (2018). Penerapan sistem kriptografi enkripsi jamak dan tanda tangan digital dalam mendukung keamanan informasi. *TEMATIKA: Journal of Informatics and Information Systems*, *6*(1), 39-46. Retrieved from

https://www.uajm.ac.id/files/journals/2/articles/83/submission/copyedit/83-156-1-CE.pdf

Darmayani, A. (2018). *SIBERPEDIA: Panduan Pintar Keamanan Siber*. Yogyakarta, Indonesia: Center for Digital Society, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Gadjah Mada.

Febrianta, M., Indrawati, I., & Amani, H. (2019, June 29). Identification of e-Governance Indicators for Measuring Smart Governance in Bandung City. https://doi.org/10.31227/osf.io/avbsu

Google Consumer Barometer. (2017a). *Do People Use The Internet For Personal Puposes*. Google Consumer Barometer. Retrieved from https://www.consumerbarometer.com/en/graph-builder/?question=N1&filter=country:indonesia

Google Consumer Barometer. (2017b). *How Often Do People Go Online (For Personal Internet Usage)*. Google Consumer Barometer. Retrieved from https://www.consumerbarometer.com/en/graph-builder/?question=M6&filter=country:indonesia

Google Consumer Barometer. (2017c). *Which Device Do People Use*. Google Consumer Barometer. Retrieved from https://www.consumerbarometer.com/en/graph-builder/?question=M1&filter=country:indonesia

Ihwani, M. (2016). Model Keamanan Informasi Berbasis Digital Signature Dengan Algoritma RSA. *Journal of Computer Engineering, Science and System*, *1*(1), 15-20. https://doi.org/10.24114/cess.v1i1.4037

Kumar, T. V. M. (2015). *E-Governance for Smart Cities*. Singapore: Springer Science+Business Media. https://doi.org/10.1007/978-981-287-287-6

Liyanti, L., & Hakim, A. R. (2019). Perancangan Penerapan Tanda Tangan Digital Sebagai Pengembangan Sistem Pelayanan Pentashihan Al Quran Digital. *SISTEMASI: Jurnal Sistem Informasi*, *8*(1), 41–54. https://doi.org/10.32520/stmsi.v8i1.415

Menezes, A. J., Oorschot, P. V. C., & Vanstone, S. A. (1997). *Handbook of Applied Cryptography (Discrete Mathematics and Its Applications)*. Florida, United States: CRC Press.

Miraz, M. H., Ali, M., Excell, P. S., & Picking, R. (2015). A review on Internet of Things (IoT), Internet of Everything (IoE) and Internet of Nano Things (IoNT). *2015 Internet Technologies and Applications (ITA)*, 219–224. Wrexham, UK. https://doi.org/10.1109/itecha.2015.7317398

Munir, R. (2015). Penggunaan Tanda-Tangan Digital untuk Menjaga Integritas Berkas Perangkat Lunak. *Prosiding SNATi2015*, F-31-F-34. Yogyakarta, Indonesia. Retrieved from https://journal.uii.ac.id/Snati/article/view/1364

Pande, D. J. (2017). *Introduction to Cyber Security*. Uttarakhand, India: Uttarakhand Open University.

Perdana, R. A., Anbiya, D. R., & Grahitandaru, A. (2019). Penerapan Tanda Tangan Digital pada Gambar Formulir C1.Plano-KWK di Pilkada Sulawesi Selatan. *Jurnal Teknologi Informasi Dan Ilmu Komputer*, *6*(5), 475–484. https://doi.org/10.25126/jtiik.2019651471

Pooja, M., & Yadav, M. (2018). Digital Signature. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *3*(6), 71-75. Retrieved from http://ijsrcseit.com/paper/CSEIT183613.pdf

Precilia, D. P., & Izzuddin, A. (2015). Aplikasi Tanda Tangan Digital (Digital Signature) Menggunakan Algoritma Message Digest 5 (MD5). *Energy*, *5*(1), 14-19. Retrieved from https://ejournal.upm.ac.id/index.php/energy/article/view/155

Selular.id. (2018, August 5). Penggunaan Tanda Tangan Digital di Indonesia Tumbuh Pesat. Retrieved from https://selular.id/2018/08/penggunaan-tanda-tangan-digital-di-indonesia-tumbuh-pesat/

Septianingrum, A., Ahmad, D., Styawan, H., Ashar, I. M., Banyumurti, I., Mardiana, Magdalena, M., Ameliah, R., & Khoiriyah, R. (2018). *Pengantar Tata Kelola Internet*. Jakarta, Indonesia: Kementerian Komunikasi dan Informatika Republik Indonesia.

---

**About the Authors**

1. **Nursani Budiarti,** a graduate student at Master of Government Science, Jusuf Kalla School of Government, Universitas Muhammadiyah Yogyakarta, Indonesia.
   E-Mail: nursani.budiarti@gmail.com

2. **Yahya Pandega Putra,** a graduate student at Master of Government Science, Jusuf Kalla School of Government, Universitas Muhammadiyah Yogyakarta, Indonesia.
   E-Mail: namakuyahya@gmail.com

3. **Achmad Nurmandi,** obtained his Doctoral degree from Universitas Indonesia, in 2008. The author is a Professor at the Department of Political Islam - Political Science, Jusuf Kalla School of Government, Universitas Muhammdiyah Yogyakarta, Indonesia.
   E-Mail: nurmandi_achmad@umy.ac.id


https://doi.org/10.33019/society.v8i2.222