Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK) DOI: 10.25126/jtiik.2023106544
Vol. 10, No. 4, Agustus 2023, hlm. 857-864 p-ISSN: 2355-7699
Akreditasi KEMENRISTEKDIKTI, No. 36/E/KPT/2019 e-ISSN: 2528-6579

ANALISIS KOMPARATIF KEAMANAN APLIKASI PENGELOLA KATA SANDI BERBAYAR LASTPASS, 1PASSWORD, DAN KEEPER BERDASARKAN ISO/IEC 25010

Whisnu Yudha Aditama[1], Ira Rosianal Hikmah[*2], Dimas Febriyan Priambodo[3]

[1, 2, 3]Politeknik Siber dan Sandi Negara, Kabupaten Bogor
Email: [1]whisnu.yudha@student.poltekssn.ac.id, [2]ira.rosianal@poltekssn.ac.id, [3]dimas.febriyan@bssn.go.id
*Penulis Korespondensi

(Naskah masuk: 13 September 2022, diterima untuk diterbitkan: 26 Juli 2023)

Abstrak

Authentikasi merupakan salah satu faktor terpenting dalam ruang lingkup keamanan komputer, penggunaan kata sandi menjadi metode autentikasi yang dominan diterapkan pada *website* ataupun desktop. Penanganan yang buruk terhadap kata sandi dapat memicu berbagai risiko seperti pencurian data sensitif, dan kerusakan reputasi, yang dapat dirasakan baik individu maupun organisasi. Aplikasi pengelola kata sandi tersedia secara gratis maupun berbayar untuk membantu pengguna dalam mengelola banyaknya kata sandi. Aplikasi pengelola kata sandi berbayar memiliki keunggulan dalam hal popularitas dan fungsi yang ditawarkan kepada pengguna. Akan teteapi banyaknya penyedia aplikasi pengelola kata sandi membuat pengguna menghadapi banyak pilihan, sehingga perlu dilakukan komparasi mengenai keamanan pada aplikasi pengelola kata sandi yang akan digunakan. Pada penelitian ini dilakukan analisis komparasi keamanan pada aplikasi pengelola kata sandi berbayar Lastpass, 1Password, dan Keeper sebagai aplikasi yang populer berdasarkan ISO/IEC 25010 untuk mengetahui kelebihan dan kekurangan dari masing-masing aplikasi. Penelitian ini merupakan penelitian kausal komparatif dengan tiga tahapan penelitian. Hasil penelitian ini adalah Aplikasi Keeper lebih unggul dalam menerapkan pencegahan kerusakan data dan kebijakan autentikasi yang diperlukan. Sedangkan, aplikasi 1Password lebih unggul dalam membuktikan identitas pengguna sebagai yang diklaim dan mampu mencatat setiap aktivitas pengguna ke dalam log. dan aplikasi Lastpass memiliki keunggulan yang sama dengan aplikasi Keeper dalam durasi menyimpan log di dalam sistem. Selain itu, ketiga aplikasi memiliki tingkat keamanan yang sama dalam mengamankan data pengguna dari otoritas tidak sah, serta menerapkan penggunaan tanda tangan atau sertifikat digital untuk mencegah terjadinya penyangkalan.

Kata kunci: *analisis komparasi, ISO/IEC 25010, kata sandi, keamanan*

COMPARATIVE ANALYSIS OF SECURITY APPLICATIONS PAID PASSWORD MANAGER LASTPASS, 1PASSWORD, AND KEEPER BASED ON ISO/IEC 25010

Abstract

Authentication is one of the most important factors in the scope of computer security, passwords are the dominant authentication method applied to websites or desktops. Poor handling of passwords can lead to various risks such as theft of sensitive data, and reputational damage, which can be felt by both individuals and organizations. Password manager apps are available both free and paid to help users manage multiple passwords. Paid password manager apps have an edge in terms of popularity and functionality offered to users. However, the many providers of password manager applications make users face many choices, so it is necessary to make a comparison regarding the security of the password manager application that will be used. In this study, a comparative security analysis was conducted on the paid password manager applications Lastpass, 1Password, and Keeper as popular applications based on ISO/IEC 25010 to determine the advantages and disadvantages of each application. This research is a comparative causal research with three stages of research. The results of this study are the Keeper application is superior in implementing data corruption prevention and authentication policies required. Meanwhile, the 1Password application is superior in proving the identity of the user as claimed and is able to log every user activity into a log. and the Lastpass application has the same advantages as Keeper application in the duration of keeping logs in the system. In addition, three applications have the same level of security in securing user data from unauthorized parties, and implement the use of digital signatures or certificates to prevent denial.

Keywords: *analisis kompatif, aplikasi pengelola kata sandi, ISO/IEC 25010, keamanan*

1. PENDAHULUAN

Saat ini, penggunaan kata sandi banyak diterapkan pada aplikasi berbasis *website*, desktop, maupun android untuk proses autentikasi (Oesch, 2021). Kata sandi berperan di garis depan sebagai pertahanan terhadap akses dari otoritas tidak sah untuk melindungi informasi pribadi pengguna. Ketika seseorang tidak menangani penggunaan kata sandi dengan benar, maka hal ini dapat menjadi faktor risiko paling signifikan dalam hal keamanan seperti terjadinya kebocoran data sensitif, kerusakan reputasi, dan penyalahgunaan data. Risiko tersebut dapat terjadi pada individu bahkan organisasi (Mccarney, 2013) (Cabarcos et al., 2016).

Aplikasi pengelola kata sandi tersedia secara gratis maupun berbayar untuk membantu pengguna dalam membuat, menyimpan, dan mengelola kata sandi (Cabarcos et al., 2016). Akan tetapi, versi gratis memiliki beberapa kelemahan seperti terbatasnya jumlah kata sandi yang bisa disimpan, hanya mendukung platform tertentu, dan tidak memiliki fungsi sinkronisasi antar perangkat. Sementara aplikasi berbayar dapat menyediakan fungsi tersebut. Hal ini menjadi keunggulan dari aplikasi pengelola kata sandi berbayar.

Banyaknya penyedia aplikasi pengelola kata sandi berbayar membuat pengguna menghadapi banyak pilihan, sehingga spesifikasi aplikasi pengelola kata sandi perlu diketahui sebagai bahan pertimbangan untuk menentukan aplikasi yang akan digunakan. Menurut Carlos Luevanos tahun 2017 Penting untuk mempertimbangkan aplikasi pengelola kata sandi apa yang akan dipilih, karena tanpa pertimbangan, pengguna berpotensi memilih aplikasi yang rentan dan dapat mengancam data pengguna itu sendiri (Luevanos et al., 2017).

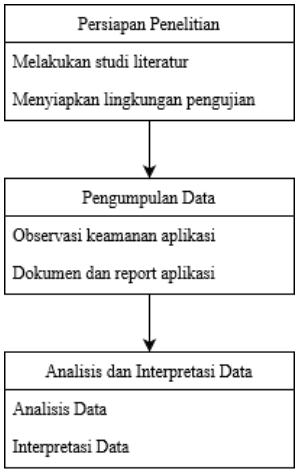
Pada penelitian ini dilakukan analisis komparasi keamanan pada beberapa aplikasi pengelola kata sandi yang paling populer tahun 2022 untuk menilai kelebihan dan kekurangan dari setiap aplikasi. Penelitian ini merupakan penelitian kausal komparatif karena membandingkan aplikasi sebagai objek yang diteliti untuk menentukan spesifikasi keamanan aplikasi.

Di antara banyaknya aplikasi pengelola kata sandi yang ada, aplikasi Lastpass, 1Password, dan Keeper menjadi aplikasi yang populer tahun 2022 atau banyak dirujuk oleh beberapa *website* dengan banyak fitur yang disediakan. Karakteristik keamanan pada penelitian ini mengacu pada ISO/IEC 25010 sebagai standar internasional yang digunakan untuk mengukur kualitas dari *system* atau *software* (Anon., 2011). Karakteristik keamanan dipilih karena menjadi karakteristik utama pada model kualitas aplikasi yang berkaitan dengan perlindungan privasi data pengguna (Anon., 2011).

Rumusan masalah pada penelitian ini adalah bagaimana hasil komparasi keamanan dari aplikasi pengelola kata sandi berbayar Lastpass, 1Password, dan Keeper berdasarkan ISO/IEC 25010. Penelitian ini diharapkan dapat digunakan sebagai informasi dan referensi dalam mempertimbangkan aplikasi pengelola kata sandi yang akan dipilih.

2. METODE PENELITIAN

Gambar 1 menyajikan alur dari penelitian ini.



Gambar 1. Alur Penelitian

Penelitian ini terbagi menjadi tiga tahapan, yaitu persiapan penelitian, pengumpulan data, analisis, dan interpretasi data.

2.1. Tahapan Persiapan Penelitian

Tahapan persiapan penelitian bertujuan untuk mencari informasi yang diperlukan untuk melakukan penelitian. Tahapan ini berisi kegiatan studi literasi, mempelajari aplikasi yang diteliti, dan menyiapkan perangkat yang digunakan dalam penelitian. Tabel 1. berisi informasi mengenai spesifikasi perangkat yang digunakan dalam penelitian.

Tabel 1. Spesifikasi Perangkat Penelitian

Model	Thinkpad Lenovo X230
OS	Windows 10 Pro 64-Bit
Processor	Intel Core i5-3320M CPU @2.60GHz (4 CPUs)
Memory	12288MB RAM

Pada penelitian ini, terdapat dua aplikasi yang digunakan untuk observasi keamanan, yaitu: Wireshark, dan Burpsuite.

2.2. Tahapan Pengumpulan Data

Tahapan pengumpulan data berisi kegiatan observasi keamanan aplikasi serta mencari informasi mengenai keamanan aplikasi dari dokumen dan *white paper* aplikasi. Berdasarkan ISO/IEC 25010 karakteristik keamanan terdiri dari lima sub karakteristik yaitu kerahasiaan, integritas, *non-repudiation*, akuntabilitas, dan keaslian (Anon., 2011).

1. Kerahasiaan

Sub karakteristik kerahasiaan digunakan untuk mengukur sejauh mana data pada sistem atau produk dapat diakses oleh pihak yang memiliki hak (Anon., 2011). Terdapat dua ukuran kualitas pada sub karakteristik kerahasiaan, yaitu:

a. *Data Encryption Correctness* untuk mengukur tingkat penerapan enkripsi dan dekripsi data. Pengumpulan data dilakukan dengan melihat isi paket yang dikirimkan oleh aplikasi ke server dan memantau penerapan enkripsi data pada aplikasi (Anon., 2011). Pengumpulan data ini dilakukan menggunakan *tools* Wireshark pada saat pengguna *login* (Aziz, Sapta and Rochimah, 2018).
b. *Strength of Cryptographic Algorithm* untuk mengukur seberapa kuat algoritma kriptografi yang digunakan. Pengumpulan data dilakukan dengan mencari informasi mengenai algoritma kriptografi yang digunakan aplikasi.

2. Integritas

Sub karakteristik integritas digunakan untuk mengukur tingkat pencegahan modifikasi sistem yang dilakukan oleh akses yang tidak diketahui (Anon., 2011). Terdapat dua ukuran kualitas pada sub karakteristik integritas, yaitu:

a. *Data Integrity Conformance* untuk mengukur tingkat pencegahan modifikasi data oleh otoritas tidak sah. Pengumpulan data dilakukan menggunakan *tools* Burpsuite dan Wireshark dengan mengeksplorasi aplikasi dalam menerapkan pencegahan terhadap risiko kerusakan data oleh otoritas tidak sah mengacu pada OWASP Top 10 *Desktop Security Risk*: *improper cryptography usage, insecure communication, dan insufficient logging & monitoring* (Aziz, Sapta and Rochimah, 2018).
b. *Internal Data Corruption Prevention* untuk mengukur metode pencegahan modifikasi data yang telah diterapkan. Pengumpulan data dilakukan dengan mengeksplorasi aplikasi dalam menerapkan *backup data*, dan menyimpan data pada beberapa tempat penyimpanan.

3. *Non-Repudiation*

Sub karakteristik *non-repudiation* digunakan untuk mengukur sejauh mana aktivitas atau *event* itu dapat dibuktikan telah terjadi, sehingga tidak dapat disangkal lagi di kemudian hari (Anon., 2011). Terdapat satu ukuran kualitas pada sub karakteristik *non-repudiation* yaitu *digital signature usage* untuk mengukur proporsi aktivitas yang memerlukan *non-repudiation* yang diproses menggunakan tanda tangan digital. Pengumpulan data dilakukan dengan mengeksplorasi penggunaan tanda tangan atau sertifikat digital mengacu pada standar X. 509 untuk memastikan bahwa tidak dapat dilakukannya penyangkalan.

4. Akuntabilitas

Sub karakteristik akuntabilitas digunakan untuk mengukur sejauh mana tindakan suatu entitas dapat ditelusuri secara unik ke entitas tersebut (Anon., 2011). Terdapat dua ukuran kualitas pada sub karakteristik akuntabilitas, yaitu:

a. *User Audit Trail Completeness* untuk mengukur kelengkapan jejak audit terkait akses pengguna ke sistem atau data. Dilakukan dengan mengobservasi aplikasi dalam mencatat log terkait aktivitas pengguna meliputi login gagal/sukses, membuat, mengubah, dan menghapus item atau kata sandi (Aziz, Sapta and Rochimah, 2018).
b. *System Log Retention* untuk mengukur durasi log sistem disimpan dalam penyimpanan yang stabil. Pengumpulan data dilakukan dengan mengobservasi sistem log dari setiap aplikasi (Aziz, Sapta and Rochimah, 2018).

5. Keaslian

Sub karakteristik keaslian digunakan untuk mengukur sejauh mana identitas subjek atau *resource* dapat dibuktikan sebagai yang diklaim (Anon., 2011). Terdapat dua ukuran kualitas pada sub karakteristik keaslian, yaitu:

a. *Authentication Mechanism Sufficiency* untuk mengukur seberapa baik sistem melakukan autentikasi identitas subjek. Pengumpulan data dilakukan dengan mengobservasi sistem *login* aplikasi dalam membuktikan identitas pengguna sebagai yang diklaim (Aziz, Sapta and Rochimah, 2018).
b. *Authentication Rules Conformity* untuk mengukur sejauh mana aplikasi menerapkan kebijakan autentikasi yang diperlukan. Pengumpulan data dilakukan dengan mengeksplorasi sistem *login* aplikasi dalam menerapkan kebijakan yang diperlukan mengacu pada OWASP Application Security Verification Standard (ASVS) 4.0 (OWASP, 2019).

2.3. Tahapan Analisis dan Interpretasi Data

Tahapan ini berisi kegiatan yang bertujuan untuk membandingkan, menganalisis, dan menginterpretasikan data yang telah diperoleh. Beberapa kegiatan yang dilakukan pada tahap ini adalah sebagai berikut:

1. Menyusun data karakteristik keamanan dari aplikasi Lastpass, 1Password, dan Keeper yang hasilnya berupa tabel untuk memudahkan visualisasi data.
2. Menganalisis data yang telah dibandingkan berdasarkan karakteristik keamanan sehingga

didapatkan hasil analisis komparasi karakteristik keamanan.
3. Interpretasi data hasil analisis komparasi untuk mempermudah penarikan kesimpulan.

3. HASIL PENELITIAN

Proses analisis dimulai dengan mengolah data yang didapatkan dari observasi keamanan aplikasi Lastpass, 1Password, dan Keeper. Berikut merupakan hasil observasi yang didapatkan pada setiap sub karakteristik keamanan:

3.1 Kerahasiaan

Berdasarkan hasil pemantauan aplikasi saat login menggunakan Wireshark dan studi literatur untuk mencari informasi mengenai model enkripsi aplikasi yang telah dilakukan pada aplikasi Lastpass, 1Password, dan Keeper, diketahui bahwa tidak terdapat perbedaan yang signifikan mengenai penerapan enkripsi maupun algoritma kriptografi yang digunakan oleh aplikasi yang diteliti. Tabel 2 berisi komparasi data dari penerapan enkripsi dan algoritma kriptografi yang digunakan aplikasi.

Tabel 2. Hasil Komparasi Kerahasiaan Aplikasi

Ukuran Kualitas	Aplikasi yang Diteliti		
	Lastpass	1Password	Keeper
Data Encryption Correctness	TLS 1.2	TLS 1.2	TLS 1.2
Strength of Cryptographic Algorithm	AES-256 (CBC) + PBKDF2-SHA256 (100.100)	AES-256 (GCM) +PBKDF2 (100.000)-HMAC-SHA256	AES-256 + PBDKF2 (100.000)

Berdasarkan tabel di atas, hasil yang didapatkan mengenai *data encryption correctness* adalah tidak terdapat data dalam bentuk teks terang yang dikirimkan oleh aplikasi Lastpass, 1Password, dan Keeper kepada server. Ketiga aplikasi mengirimkan data melalui TLS versi 1.2. Hal ini menunjukkan bahwa ketiga aplikasi menerapkan enkripsi data dengan baik.

Kemudian hasil yang didapatkan mengenai *strength of cryptographic algorithm* adalah ketiga aplikasi menggunakan algorithma AES-256 bit untuk mengenkripsi data pengguna. Perbedaan algoritma enkripsi dari ketiga aplikasi terletak pada mode, jumlah *round* pada PBKDF, dan fungsi *hash* yang digunakan. Hal ini menunjukkan bahwa ketiga aplikasi menggunakan algoritma yang kuat untuk mengenkripsi data pengguna.

3.2 Integritas

Setelah dilakukan observasi mengenai penerapan pencegahan kerusakan data baik yang disebabkan oleh internal maupun eksternal pada aplikasi Lastpass, 1Password, dan Keeper, didapatkan hasil komparasi seperti pada Tabel 3.

Berdasarkan tabel 3, dapat diketahui bahwa aplikasi Keeper menerapkan tiga pencegahan kerusakan data yang disebabkan oleh pihak eksternal, sedangkan aplikasi Lastpass dan 1Password tidak menerapkan pencegahan kerusakan data pada *file* log aplikasi, sehingga aplikasi tersebut tidak dapat menjamin integritas dari log yang ditampilkan.

Selanjutnya hasil yang didapatkan mengenai metode pencegahan kerusakan data yang diterapkan aplikasi adalah aplikasi 1Password dan Keeper menerapkan fungsi *backup* data dengan menyediakan fungsi *import/export*, sehingga pada saat terjadi kerusakan data, maka data tersebut dapat dipulihkan menggunakan *file backup*. Selain itu, ketiga aplikasi menyimpan data pengguna pada beberapa tempat penyimpanan yaitu penyimpanan lokal, dan penyimpanan *cloud*.

3.3 Non-Repudiation

Setelah melakukan observasi menggunakan *tools* Wireshark pada aplikasi Lastpass, 1Password, dan Keeper, diketahui bahwa tidak terdapat perbedaan yang signifikan mengenai penggunaan tanda tangan atau sertifikat digital pada aplikasi ketiga aplikasi yang diteliti. Tabel 4 menyajikan hasil komparasi data dari penggunaan tanda tangan atau sertifikat digital pada aplikasi Lastpass, 1Password, dan Keeper.

Berdasarkan Tabel 4. didapatkan hasil bahwa ketiga aplikasi menggunakan sertifikat digital versi tiga. Algoritma kriptografi yang digunakan oleh ketiga aplikasi adalah algoritma kriptografi yang sama yaitu RSA 2048-bit dengan fungsi hash SHA-256.

Perbedaan dari ketiga sertifikat tersebut adalah Aplikasi 1Password dan Keeper diterbitkan oleh Amazon dengan periode validitas yang lebih singkat dibandingkan dengan aplikasi Lastpass yang diterbitkan oleh GlobalSign dengan periode validitas selama satu tahun.

3.4 Akuntabilitas

Berdasarkan pengumpulan data yang telah dilakukan pada aplikasi Lastpass, 1Password dan Keeper terdapat perbedaan mengenai kelengkapan jejak audit pengguna dan durasi waktu *log* disimpan pada aplikasi. Data tersebut didapatkan dari hasil eksplorasi sistem *log* dari aplikasi yang diteliti. Tabel 5 menyajikan komparasi data dari kelengkapan jejak audit dan durasi waktu log disimpan pada aplikasi.

Tabel 3. Hasil Komparasi Integritas Aplikasi

Risiko/Metode	Aplikasi yang Diteliti		
	Lastpass	**1Password**	**Keeper**
Data Integrity Conformance			
Improper Cryptography Usage	HMAC dengan algoritma AES-256_GCM_SHA384	HMAC dengan algoritma AES-128_GCM_SHA256	HMAC dengan algoritma AES-128_GCM_SHA256
Insecure Communication	GlobalSign Root CA HTTPS	Amazon Root CA HTTPS	Amazon Root CA HTTPS
Insufficient Logging & Monitoring	Tidak menerapkan restriksi pada *file log*	Tidak menerapkan restriksi pada *file log*	*Log* tidak dapat diubah oleh pengguna
Internal Data Corruption Prevention			
Backup data	Tidak menerapkan ekspor data	Menyimpan ekspor data dalam format 1PUX atau CSV	Menyimpan ekspor data dalam format CSV, JSON atau PDF
Stored data in multiple sites	*Local* dan *Cloud*	*Local* dan *Cloud*	*Local* dan *Cloud*

Tabel 4. Hasil Komparasi *Non-Repudiation* Aplikasi

Aspek	Aplikasi yang Diteliti		
	Lastpass	**1Password**	**Keeper**
Version	3	3	3
Serial Number	25f3971581db3626094bc2e4	0c4e773b04a0b7b6fdffb9728c434ed4	08ec24aaf7492b99743c6e663f9c22b7
Signature Algorithm ID	1.2.840.113549.1.1.11	1.2.840.113549.1.1.11	1.2.840.113549.1.1.11
Issuer Name	GlobalSign Extended Validation CA	Amazon	Amazon
Validity Period	2 Tahun	1 Tahun	1 Tahun
Subject Name	lastpass.com	1password.com	Keepersecurity.com
Subject Public Key	RSA Encryption 2048-bit	RSA Encryption 2048-bit	RSA Encryption 2048-bit
Extentions	10 ekstensi	10 ekstensi	10 ekstensi
Signature	SHA256 With RSA *Encryption*	SHA256 With RSA *Encryption*	SHA256 With RSA *Encryption*

Berdasarkan Tabel 5, hasil yang didapatkan mengenai *user audit trail completeness* adalah aplikasi Lastpass hanya mencatat aktivitas *login* gagal yang dilakukan oleh pengguna, sedangkan aplikasi 1Password mencatat setiap aktivitas pengguna pada *file* log aplikasi. Aplikasi Keeper mencatat aktivitas *login* sukses, membuat, mengubah, dan menghapus item aplikasi. Hal ini menunjukkan bahwa aplikasi 1Password lebih unggul dalam menelusuri riwayat aktivitas pengguna dibandingkan aplikasi Lastpass dan Keeper.

Selanjutnya, hasil yang didapatkan mengenai *system log retention* adalah aplikasi Lastpass dan Keeper menyimpan riwayat log di dalam sistem masing-masing sejak aplikasi tersebut dipasang, sedangkan aplikasi 1Password menyimpan *file* log aplikasi selama 14 hari. Hal ini menunjukkan bahwa aplikasi Lastpass dan Keeper lebih unggul dalam menyimpan data log.

Tabel 5 Hasil Komparasi Akuntabilitas Aplikasi

Aspek	Aplikasi yang Diteliti		
	Lastpass	1Password	Keeper
User Audit Trail Completeness			
Login gagal	Tercatat	Tercatat	Tidak Tercatat
Login Sukses	Tidak Tercatat	Tercatat	Tercatat
Membuat Item	Tidak Tercatat	Tercatat	Tercatat
Mengubah Item	Tidak Tercatat	Tercatat	Tercatat
Menghapus Item	Tidak Tercatat	Tercatat	Tercatat
System Log Retention			
Waktu Log Disimpan	Lifetime	14 Hari	Lifetime

3.5 Keaslian

Berdasarkan pengumpulan data yang telah dilakukan pada aplikasi Lastpass, 1Password dan Keeper terdapat perbedaan mengenai penerapan metode autentikasi dan kebijakan autentikasi pada masing-masing aplikasi. Data tersebut didapatkan dari hasil observasi sistem login dari aplikasi yang diteliti. Data tersebut dapat dilihat pada Tabel 4.6 yang menyajikan hasil komparasi metode autentikasi yang tersedia dan kebijakan autentikasi yang diterapkan.

Tabel 6 Hasil Komparasi Keaslian Aplikasi

Metode/Aspek	Aplikasi yang Diteliti		
	Lastpass	1Password	Keeper
Authentication Mechanism Sufficiency			
Text Password	1	1	1
ID-Based	1	-	2
Mobile-Based	1	-	-

Metode/Aspek	Aplikasi yang Diteliti		
	Lastpass	1Password	Keeper
Windows Hello	1	1	1
Text Passwords AND ID-Based	2	1	-
Text Passwords AND OTP	6	1	2
ID Based AND Text Password	-	2	-
Secret Key AND Text Password	-	1	-
Text Passwords AND Biometrics	1	-	-
Text Passwords AND Mobile-Based	-	-	2
Secret Key AND Text Password AND ID-Based	-	1	-
ID-Based AND Text Password AND OTP	-	2	-
ID-Based AND Text Password AND ID-Based	-	2	-
Jumlah	**13**	**13**	**8**
Authentication Rules Conformity			
Password Security Requirements	9	8	10
General Authenticator Requirements	3	2	3
Authenticator Lifecycle Requirements	1	1	1
Credential Recovery Requirements	5	3	5
Out of Band Verifier Requirements	3	3	3
Single or Multi Factor One Time Verifier Requirements	1	1	1
Total Kebijakan yang Diterapkan	22	18	23
Total Kebijakan yang diperlukan	27	27	27

Berdasarkan Tabel di atas, hasil yang didapatkan mengenai *authentication mechanism sufficiency* adalah aplikasi Lastpass dan 1Password menyediakan 13 metode autentikasi kepada pengguna, dimana pada aplikasi Lastpass terdapat empat metode *one-factor authentication*, dan sembilan metode *two-factor authentication*, sedangkan pada aplikasi 1Password, terdapat dua metode *one-factor authentication*, lima metode *two-factor authentication* dan enam metode *three-factor authentication*. Aplikasi Keeper menyediakan delapan metode autentikasi yang terdiri dari empat metode *one-factor authentication*, dan empat metode *two-factor authentication*. Hal ini menunjukkan bahwa aplikasi Lastpass dan 1Password lebih unggul dalam menyediakan kombinasi metode autentikasi kepada pengguna. Selain itu, aplikasi 1Password lebih unggul dibanding aplikasi Lastpass dan Keeper dalam menyediakan kekuatan metode autentikasi.

Hasil yang didapatkan mengenai *authentication rules conformity* adalah aplikasi Lastpass menerapkan 22 kebijakan autentikasi, sedangkan aplikasi 1Password menerapkan 18 kebijakan autentikasi, dan aplikasi Keeper menerapkan 23 kebijakan autentikasi dari 27 kebijakan autentikasi berdasarkan OWASP ASVS 4.0 level 1. Hal ini menunjukkan bahwa aplikasi Keeper lebih unggul dalam menerapkan kebijakan autentikasi untuk memenuhi standar kualitas aplikasi berdasarkan ISO/IEC 25010.

4. KESIMPULAN DAN SARAN

Pada penelitian ini telah dilakukan analisis komparatif keamanan yang terdiri dari sub karakteristik kerahasiaan, integritas, *non-repudiation*, akuntabilitas, dan keaslian terhadap aplikasi pengelola kata sandi berbayar Lastpass, 1Password, dan Keeper Berdasarkan ISO/IEC 25010 menggunakan metode kausal komparatif dengan diperoleh kesimpulan sebagai berikut:

a. Aplikasi Keeper lebih unggul dalam menerapkan kebijakan autentikasi yang diperlukan dan pencegahan kerusakan data baik internal maupun eksternal.
b. Aplikasi 1Password lebih unggul dalam membuktikan identitas pengguna sebagai yang diklaim dan mampu mencatat setiap aktivitas pengguna ke dalam log.
c. Aplikasi Lastpass memiliki keunggulan yang sama dengan aplikasi Keeper dalam hal durasi menyimpan log di dalam sistem.
d. Selain itu, ketiga aplikasi memiliki tingkat keamanan yang sama dalam mengamankan data pengguna dari otoritas tidak sah, serta menerapkan penggunaan tanda tangan atau sertifikat digital untuk mencegah terjadinya penyangkalan.

DAFTAR PUSTAKA

ANON. 2011. *ISO/IEC 25010 Systems and software engineering- Systems and software Quality Requirements and Evaluation (SQuaRE)-System and software quality models*. 1th ed. Switzerland: ISO/IEC.

AZIZ, M.N., SAPTA, I.M. and ROCHIMAH, S., 2018. Security Characteristic Evaluation Based on ISO/IEC 25023 Quality Model, Case Study: Laboratory Management Information System. *2018 Electrical Power, Electronics, Communications, Controls and Informatics Seminar, EECCIS 2018*, pp.332–336. https://doi.org/10.1109/EECCIS.2018.8692982 .

CABARCOS, P.A., MARIN, A., PALACIOS, D., ALMENAREZ, F. and DIAZ-SANCHEZ, D., 2016. Comparing Password Management Software: Toward Usable and Secure Enterprise Authentication. *IT Professional*, [online] 18(5), pp.34–40. https://doi.org/10.1109/MITP.2016.81.

LUEVANOS, C., ELIZARRARAS, J., HIRSCHI, K. and YEH, J.H., 2017. Analysis on the security and use of password managers. In: *Parallel and Distributed Computing, Applications and*

Technologies, PDCAT Proceedings. IEEE Computer Society. pp.17–24. https://doi.org/10.1109/PDCAT.2017.00013.

MCCARNEY, D., 2013. *Comparative Evaluation, Design, Implementation and Empirical Analysis*. Ontario.

OESCH, T.S., 2021. *An Analysis of Modern Password Manager Security and Usage on An Analysis of Modern Password Manager Security and Usage on Desktop and Mobile Devices Desktop and Mobile Devices*. [online] Knoxville. Available at: <https://trace.tennessee.edu/utk_graddiss/6670/> [Accessed 13 September 2022].

OWASP, 2019. Application Security Verification Standard. (October), p.47.

Halaman ini sengaja dikosongkan