Tinjauan Keamanan pada Google Sign-in Terintegrasi

Randy Christian Saputra – 18217006 (ITB)

***Abstract*—Sejumlah aplikasi telah mengintegrasikan fitur *login* yang mereka miliki dengan fasilitas *Single Sign-On* yang disediakan pihak ketiga. Fasilitas ini mempermudah pengguna karena tidak perlu membuat dan mengingat kata sandi yang berbeda-beda untuk setiap aplikasi. Meskipun demikian, fitur ini hadir dengan sejumlah risiko. Makalah ini menganalisis setiap risiko keamanan yang ditimbulkan oleh adanya fitur *Single Sign-On* tersebut.**

***Keywords*—single sign-on, keamanan web, autentikasi**

I. PENDAHULUAN

Saat ini banyak aplikasi yang dapat diakses melalui jaringan internet melakukan autentikasi menggunakan nama pengguna (*username*) dan kata sandi. Dalam praktiknya, jika seorang pengguna ingin dirinya aman, ia harus membuat kata sandi yang berbeda-beda untuk setiap aplikasi di mana ia terdaftar. Ini menjadi kesulitan, khususnya bagi pengguna yang mempunyai kesulitan dalam menghafal. Terdapat beberapa aplikasi yang bahkan mempunyai persyaratan yang rumit bagi kata sandi. Jika pengguna sudah terlanjur membuat kata sandi sepanjang 8 karakter untuk suatu aplikasi, membuat kata sandi untuk aplikasi lainnya yang mensyaratkan kata sandi minimal 12 karakter akan menambah kesulitan pengguna dalam menghafal.

Single Sign-On adalah skema autentikasi yang mengizinkan pengguna untuk *log in* dengan satu nama pengguna dan kata sandi pada sistem peranti lunak baik yang terkait maupun independent [1]. Sejumlah manfaat yang dapat diterima pengguna dari *Single Sign-On* adalah pengalaman pengguna dalam berpindah layanan menjadi lebih aman dan tidak terganggu tanpa harus menyebutkan kredensial setiap saat. Manfaat lain yang ditawarkan adalah keamanan karena *Single Sign-On* membuat kredensial tidak tersimpan pada layanan yang diakses. Sebagai gantinya, kredensial ini hanya terdapat pada *server* SSO. Selain itu, SSO membuat pengembang piranti lunak menghemat waktu dan tenaga dalam mengembangkan piranti lunaknya karena hanya perlu mengimplementasikan skema autentikasi yang sudah disediakan [2].

Fitur *Single Sign-On* dihadirkan oleh sejumlah media sosial, seperti Facebook, Twitter, Google, LINE, dan masih banyak lagi. Dari 5 *startup unicorn* di Indonesia, terdapat 3 *startup* yaitu Bukalapak, Tokopedia, dan Traveloka yang mengimplementasikan *Single Sign-On* milik Facebook dan Google.

Selain manfaat yang diberikan, nyatanya fitur *Single Sign-On* merupakan fitur yang mempunyai risiko keamanan. Yulia Cherdantseva dan Jeremy Hilton pada *paper* yang berjudul “Understanding Information

Assurance and Security" menyimpulkan bahwa keamanan mempunyai definisi yang berbeda-beda. Untuk lingkungan data yang tidak hanya bisa diakses dari lokal, keamanan informasi perlu didefinisikan dalam sebuah kesepakatan yang disetujui Bersama [3].

Meskipun demikian, terdapat beberapa definisi berikut:

Tabel 1: Definisi Keamanan Informasi dan Integritas [3]

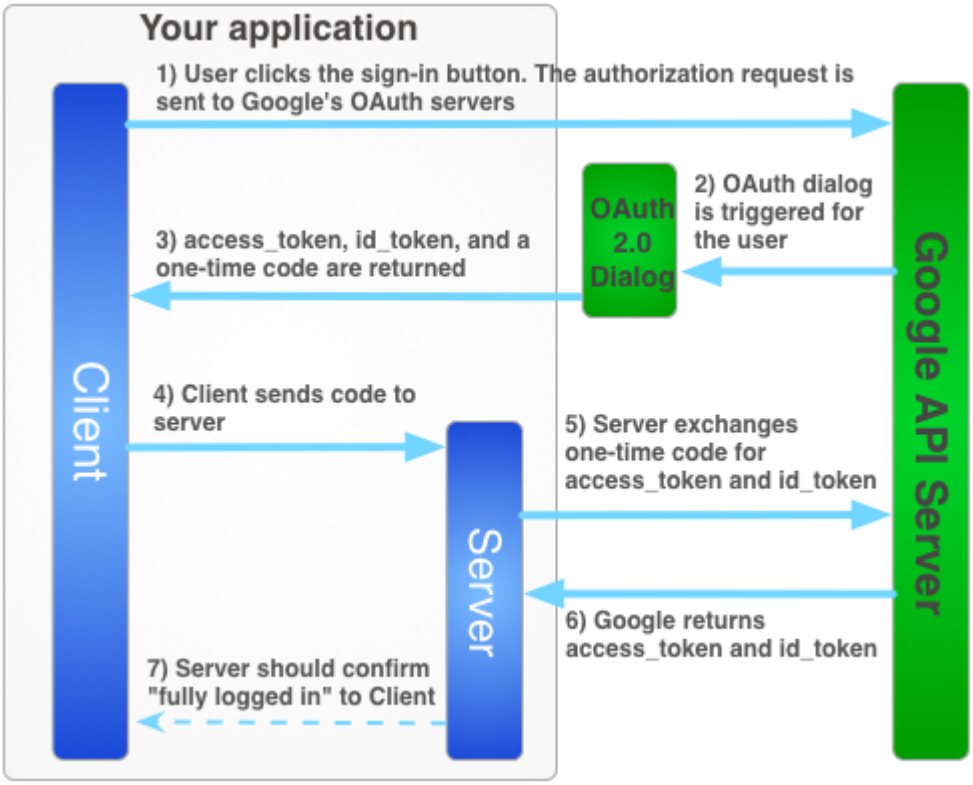
Standar	Keamanan Informasi	Integritas (*Integrity*)
ISO27000 (2009)	Menjaga kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) dari informasi. Sebagai catatan tambahan, aspek lainnya, seperti autentikasi, akuntabilitas, *non-repudiation*, dan keandalan mungkin termasuk.	Sifat (*properties*) melindungi akurasi dan kelengkapan dari asset.
CNSS (2010)	Perlindungan informasi dan sistem informasi dari akses, penggunaan, pembocoran, gangguan, modifikasi, atau perusakan yang tidak diizinkan dalam rangka menyediakan kerahasiaan, integritas, dan ketersediaan.	Sifat (*properties*) di mana sebuah entitas tidak dimodifikasi dengan tidak sah.
ISACA (2008)	Memastikan hanya pengguna yang diizinkan (kerahasiaan) yang memiliki akses pada informasi yang akurat dan lengkap (integritas) ketika dibutuhkan (ketersediaan).	Akurasi, kelengkapan, dan validitas informasi.

Sehingga berdasarkan definisi-definisi tersebut, acuan definisi keamanan yang akan digunakan pada makalah ini adalah kerahasiaan informasi (bagaimana Google menjaga kerahasiaan data pengguna), integritas data (bagaimana Google memastikan bahwa data yang diterima adalah lengkap dan tidak dimanipulasi), dan ketersediaan layanan (di mana layanan Google dapat diakses dan seberapa sering *downtime* terjadi).

II. TINJAUAN SISTEM

A. *Cara Kerja*

Sebelum membahas mengenai keamanan dari fitur *sign in* terintegrasi yang dikelola Google, perlu diketahui cara kerja dari fitur *sign in with Google* itu sendiri.



Gambar 1. Alur Informasi Pada Google *Sign-In* Terintegrasi [4]

Awalnya sebuah aplikasi web akan mendaftarkan aplikasinya pada Google terlebih dahulu. Setelah mempnyai ID aplikasi dan melakukan pemasangan integrasi *sign in* dengan Google, maka pengguna yang menekan tombol tersebut akan mengirimkan permintaan autentikasi terlebih dahulu kepada API Google yang terletak di apis.google.com. Setelah itu Google akan mengarahkan pengguna untuk memberikan *consent* atas aksi *login* tersebut, termasuk penjelasan mengenai informasi apa saja yang akan dibagikan kepada pihak ketiga (dalam hal ini perusahaan yang mengintegrasikan sistemnya dengan Google), yaitu melalui tampilan antarmuka OAuth 2.0 yang terletak di accounts.google.com. Tampilan permintaan izin untuk membagikan data ini hanya Google mungkin memberikan tantangan tambahan bagi pengguna untuk memvalidasi dirinya sendiri, misalnya dengan *One Time Password* berbasis SMS atau telepon, pertanyaan keamanan, validasi melalui *2-Step Verification phone prompts*, *time based* OTP (TOTP) menggunakan Google Authenticator, atau *backup codes*. Setelah *login* berhasil, Google akan memberikan data *token*. *Token* ini berisi informasi seperti:

- Tipe *token*, dalam hal ini yang digunakan adalah “Bearer”
- *Access token* berisi token akses OAuth 2.0
- *Scope* berisi cakupan data yang dapat diakses oleh aplikasi pihak ketiga tersebut termasuk akses apa yang diberikan pengguna kepada aplikasi tersebut
- *login_hint* berisi subjek dari autentikasi yang dilakukan, bisa berupa alamat email pengguna atau *string* yang setara dengan Google ID pengguna
- *expires_in* atau masa berlaku token yang dikirimkan (nilai *default* adalah 1 jam atau 3600 detik)
- *id_token* berisi token dalam format JWT
- parameter-parameter lainnya

Contoh dari data yang dikembalikan Google adalah sebagai berikut:


```
  {"token_type":"Bearer","access_token":"ya29.a0AfH6SMA4RXUWX7petRd2El47NMg
l3lkEXhjHpaPUxlj3Z3eXY22y85Mc57zqIEmePM-kyRa8NPL2yqRtA1ufK4Yu4Ojjogi-
v5jH149iGfdKJoi1UVbFDcOsh7jHBAxTON3dhyFwvOfibfhayECUi1kSECGinRsNheZUeZHcvjG
Buw","scope":"email profile https://www.googleapis.com/auth/userinfo.email
openid
https://www.googleapis.com/auth/userinfo.profile","login_hint":"AJDLj6J395W
yt8goKSwJUl8nAU8TQfM_58YO26KHN1MfExmIIKvj5kLF-
4O7blFs0XLAtjrYaU7PBhsBiWexkO4XYsMNAnQgnA","expires_in":3599,"id_token":"[R
EDACTED]","session_state":{"extraQueryParams":{"authuser":"0"}}}
```


Dari informasi-informasi tersebut, id_token yang berformat JWT dikirimkan kepada *server* aplikasi web untuk divalidasi. Pada saat tulisan ini dibuat, id_token adalah sebuah *token* dengan format JWT (JSON Web Token) dengan algoritma RS256 (RSA – SHA256). Aplikasi web dapat memilih 2 cara untuk melakukan validasi yaitu:

1. Mengunduh kunci publik milik Google dan melakukan validasi mandiri. Kunci publik ini dapat diakses secara bebas melalui https://www.googleapis.com/oauth2/v3/certs. Kunci publik ini diubah secara berkala, sehingga pemilik aplikasi web yang akan melakukan validasi mandiri diharapkan memperhatikan masa berlaku kunci publik melalui *response header cache-control*. Verifikasi dilakukan dengan mendekripsi *signature* pada JWT dengan kunci publik kemudian membandingkan hasilnya dengan hasil dari *hash* SHA256 terhadap *header* dan *payload*.
2. Memanggil *endpoint* tokeninfo. Endpoint ini terletak di https://oauth2.googleapis.com/tokeninfo. Token berupa id_token dikirimkan sebagai parameter

GET. Jika token tidak valid, hasilnya akan berupa error. Sebaliknya jika token valid, pastikan parameter aud dari *token* tersebut menuliskan *client ID* dari aplikasi yang didaftarkan.

3. Menggunakan mekanisme OAuth 2.0 sesuai spesifikasi Google.

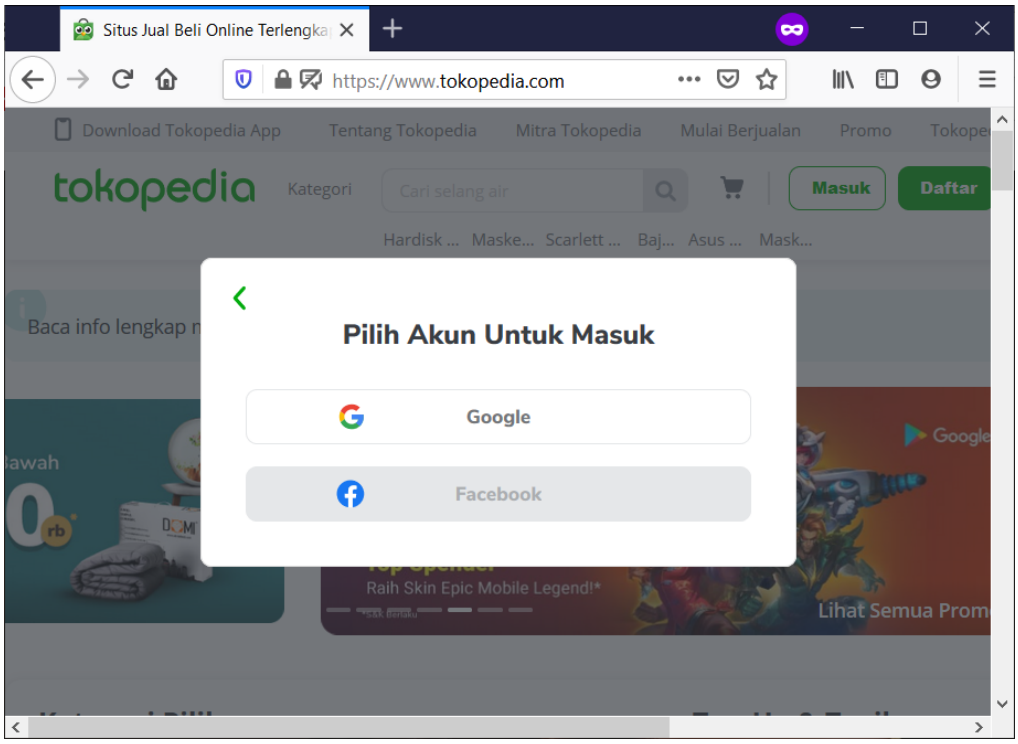
Jika token sudah dipastikan valid, aplikasi web dapat membaca *payload* dari JWT dan meyakinkan bahwa pengguna yang tercantum dalam *payload* tersebut sudah memvalidasi dirinya sendiri.

B. Confidentiality

Membahas mengenai kerahasiaan data, perlu diperhatikan terlebih dahulu adalah kebijakan yang diterapkan Google mengenai kebijakan perlindungan data pengguna. Dari sisi kebijakan secara formal, Google mempunyai kebijakan privasi yang dapat diakses melalui *footer* setiap halaman Google. Pada segmen "Membagikan informasi Anda", Google merinci kepada siapa data pengguna dibagikan. Adapun pihak yang menerima akses atas informasi pengguna adalah sebagai berikut [6]:

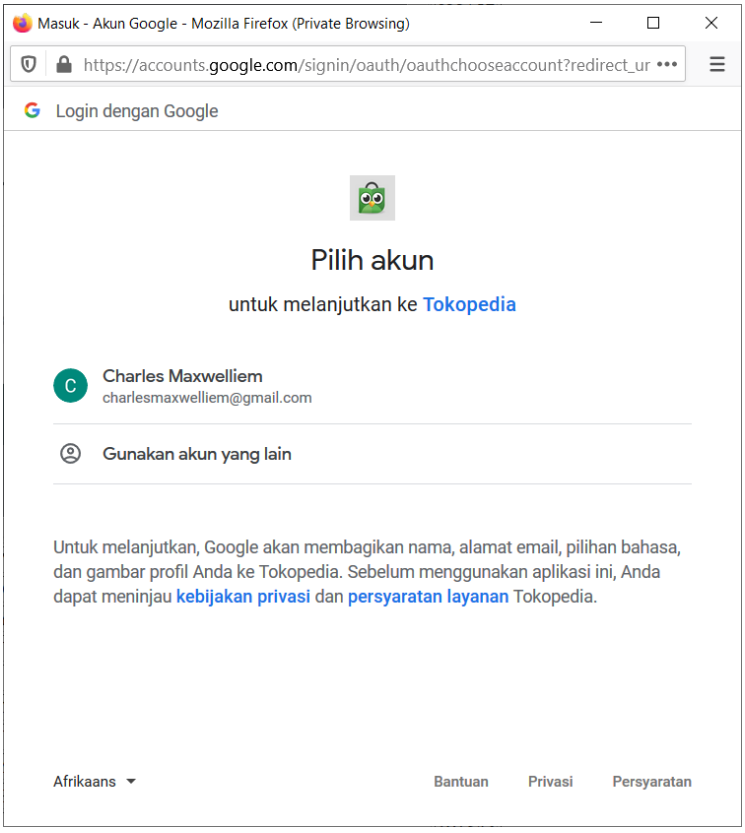
- Pihak internal Google
- Pihak yang diizinkan pengguna–Pengguna akan diminta izin secara eksplisit sebelum data dapat diakses pihak ketiga.
- Pengelola administrator domain–Dalam hal ini jika pengguna terdaftar sebagai karyawan atau pelajar dari organisasi yang menggunakan layanan Google (seperti G Suite), administrator domain dan *reseller* di mana pengguna tersebut terdaftar memiliki akses terhadap informasi akun pengguna tersebut.
- Afiliasi dan/atau bisnis atau orang terpercaya lainnya yang memproses data untuk Google, sesuai instruksi Google dan tunduk pada kebijakan privasi Google serta kerahasiaan dan langkah keamanan lain yang sesuai.
- Pihak yang berwenang–Dalam hal ini Google memberikan data pengguna kepada otoritas yang berwenang dalam rangka mematuhi hukum, peraturan, dan proses hukum yang berlaku atau permintaan pemerintah yang wajib dipenuhi. Google akan memberikan notifikasi kepada pengguna yang terdampak kecuali tuntutan hukum melarang hal tersebut.

Makalah ini secara spesifik akan membahas mengenai pembagian data kepada pihak ketiga yang diizinkan secara eksplisit oleh pengguna.



Gambar 2. Opsi Login Google di Tokopedia

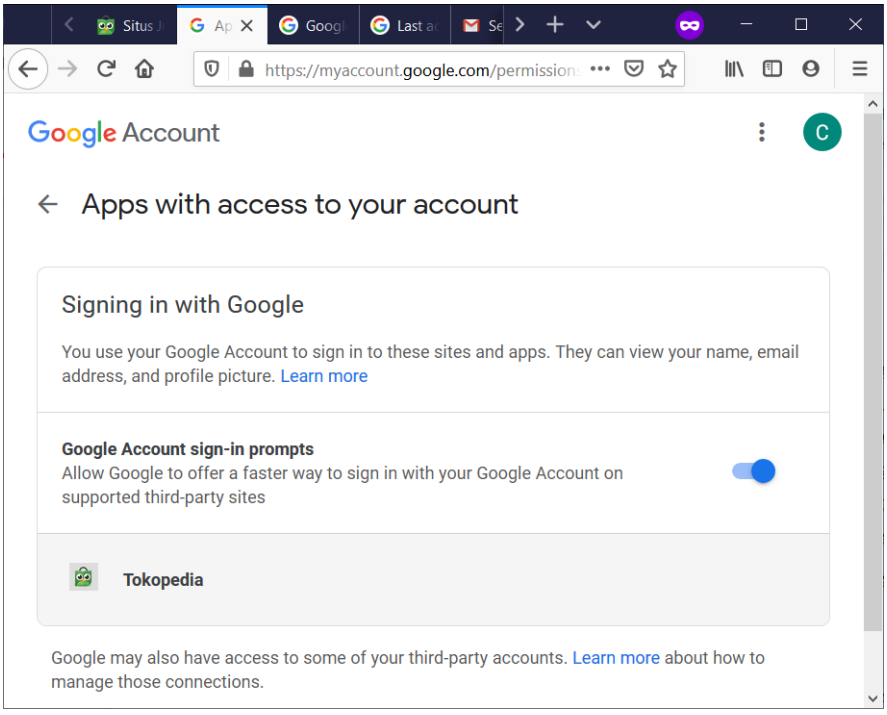
Dalam percobaan yang saya lakukan pada situs Tokopedia, pada saat tombol “Google” ditekan, muncul sebuah jendela baru untuk memilih akun yang akan digunakan untuk masuk.



Gambar 3. Layar Pemilihan Akun Pada OAuth Google

Apabila penyedia aplikasi *web* hanya meminta informasi dasar seperti nama dan alamat email, maka ketika pengguna menekan akun yang mereka ingin gunakan, pengguna akan langsung dialihkan kembali ke halaman *web* sebelumnya dan masuk sebagai pengguna yang sebelumnya dipilih. Sebaliknya jika ternyata penyedia aplikasi *web* meminta akses tambahan seperti akses terhadap data *file* Google Drive milik pengguna, maka pengguna akan diarahkan ke sebuah tampilan khusus yang menampilkan izin apa saja yang diminta oleh penyedia aplikasi *web* [5]. Pengguna memiliki hak untuk memberikan izin tersebut.

Selain itu, Google menyediakan tampilan pengaturan pengguna yang mengizinkan pengguna untuk melihat di mana saja pengguna pernah menggunakan fitur *sign in* menggunakan Google. Informasi ini disertai dengan tombol untuk menghapus akses tersebut. Nyatanya data tersebut tidak terhapus dari basis data aplikasi *web* yang bersangkutan. Ini hanya membatalkan *access token* terhadap aplikasi tersebut sehingga *access token* tidak bisa digunakan kembali untuk mendapatkan data pengguna. Apabila situs web menggunakan token berbasis JWT yang diberikan Google, maka fitur *revoke access* menjadi tidak ada gunanya.



Gambar 4. Layar Informasi Aplikasi dengan Akses Data Pengguna

Dalam hal ini, Google telah menjalankan tugasnya dengan baik dalam menjelaskan kepada siapa data dibagikan. Google juga mewajibkan pengelola aplikasi *web* yang ingin mengintegrasikan sistemnya dengan Google untuk mempunyai kebijakan privasi yang dipublikasikan di situs *web* masing-masing, sehingga pengguna dapat membaca informasi tersebut.

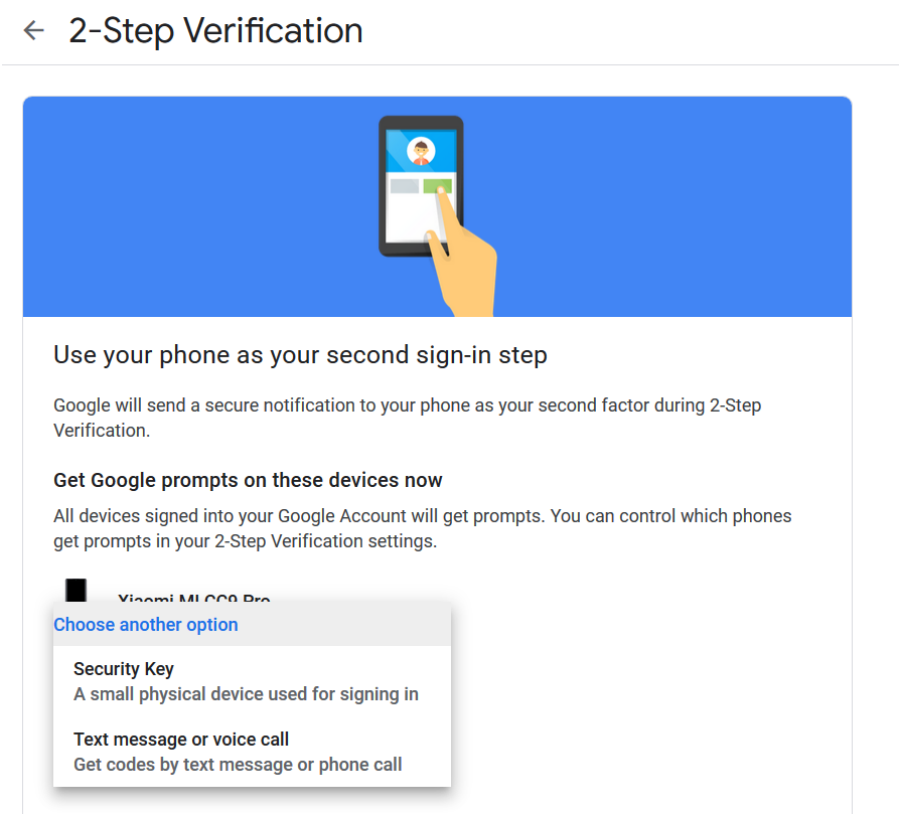
Sebagai catatan, Google mengaku telah menerapkan beberapa kebijakan untuk melindungi pengguna seperti menerapkan aturan penamaan aplikasi yang harus unik, membuat sebuah sistem yang menganalisis risiko dari sebuah aplikasi *web* dan menerapkan pengecekan manual (*manual review*) terhadap aplikasi *web* yang berpotensi menyalahgunakan data pengguna [7].

Sebagai rekam jejak, pada Maret 2018, Google menemukan dan memperbaiki celah keamanan pada API produk Google+. Pada saat itu, Google tidak dapat mengonfirmasi pengguna mana yang terdampak atas kerentanan ini dikarenakan Google hanya mempunyai *log* akses atas API produk Google+ selama 2 minggu. Meskipun demikian, Google mengklaim berdasarkan hasil analisis terhadap *log* selama 2 minggu, 500.000 akun Google+ mungkin terdampak, meskipun tidak dapat menentukan apakah data pengguna disalahgunakan. Sesuai kebijakan GDPR yang saat itu belum berlaku, Google menginformasikan kerentanan ini kepada setiap pengguna yang berpotensi terdampak [8].

C. *Integrity*

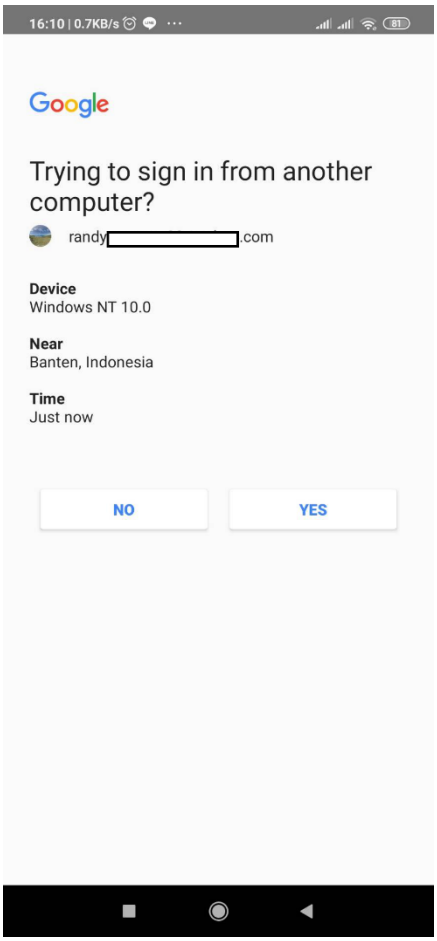
Google tidak merinci mengenai proses *login* akun Google, termasuk prosedur yang saat ini diterapkan untuk memastikan pengguna adalah pengguna yang benar dan tidak dimanipulasi.

Google menyediakan *2-Step Verification* yang bersifat opsional.



Gambar 5. Pilihan *2-step Verification* Google

Terdapat 3 metode yang ditawarkan Google untuk *2-step verification* yaitu *phone prompts*, *security key*, maupun OTP yang dikirim melalui SMS atau telepon. *Phone prompts* adalah metode verifikasi di mana pengguna akan menerima sebuah tampilan layar di *smartphone* yang tertaut dengan akun Google tersebut mengindikasikan bahwa pengguna melakukan *login*. Pengguna diberikan pilihan untuk mengizinkan atau menolak aktivitas *login* tersebut.



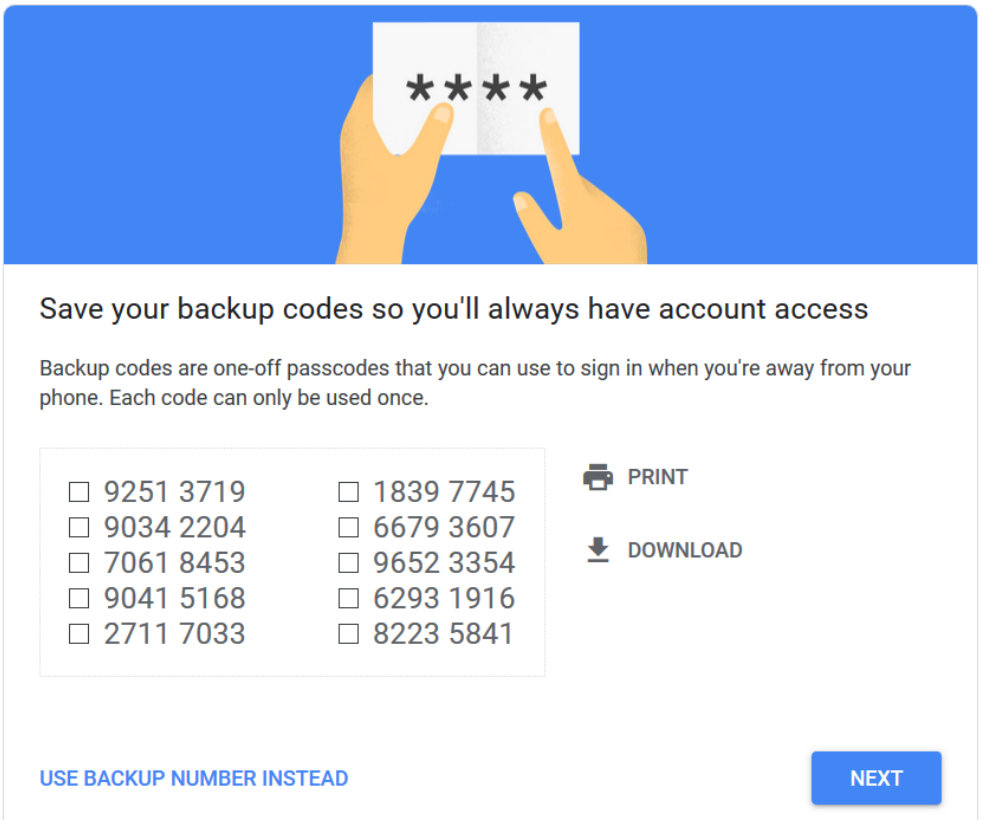
Gambar 6. *Phone Prompts* Pada Perangkat Android

Security key adalah sebuah *dongle* berukuran kecil yang dapat dibeli untuk membuktikan kegiatan *sign in*. Saat Google butuh memverifikasi identitas pengguna, pengguna dapat menghubungkan *dongle* tersebut dengan ponsel, tablet, atau computer. Google mengklaim *security key* adalah salah satu metode verifikasi paling aman untuk masuk ke akun Google [13].

Verifikasi selanjutnya adalah melalui kode OTP yang dikirimkan melalui SMS maupun telepon. Kode ini berupa 6 digit angka yang berbeda. Google tidak menjelaskan metode pembuatan kode ini apakah menggunakan HOTP ataupun TOTP ataupun metode lainnya.

Di luar ketiga metode verifikasi primer tersebut, Google juga mengizinkan penambahan 3 alternatif metode verifikasi lainnya yaitu kode cadangan, kode dari aplikasi *authenticator*, dan ponsel cadangan.

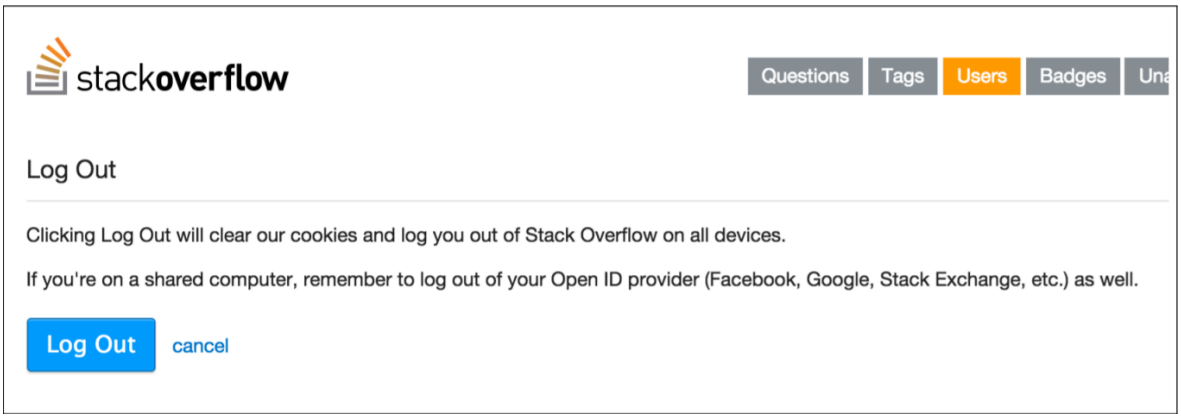
Metode ini adalah alternatif sehingga metode *2-step verification* primer harus diaktifkan minimal 1 sebelum mengaktifkan cadangannya.



Gambar 7. Kode Cadangan

Gambar 7 adalah contoh kode cadangan yang merupakan metode alternatif dalam verifikasi identitas pengguna. Satu kode cadangan hanya dapat digunakan 1 kali dan pengguna hanya dapat memiliki paling banyak 10 kode cadangan dalam 1 waktu. Apabila kode cadangan bocor ke tangan pihak lain atau kode cadangan habis, pengguna dapat meminta Google untuk menghasilkan 10 kode cadangan yang baru dan kode cadangan yang lama tidak lagi bisa digunakan.

Meskipun demikian, Vaibhav Rastogi dan Ankit Agrawal menuliskan Google tidak menyediakan fasilitas kepada pengembang aplikasi *web* untuk melakukan *single sign off*. *Single sign off* merupakan sebuah fitur yang diterapkan sejumlah pengembang *single sign on* sehingga pengguna dapat melakukan *sign out* dari akun aplikasi *web* maupun di akun penyedia *single sign on* tersebut. Ini menciptakan kebingungan tersendiri bagi pengguna di mana pengguna bisa saja berpikir bahwa ia sudah keluar dari Google hanya dengan menekan tombol keluar pada aplikasi *web* di mana pengguna tersebut melakukan aktivitasnya. Beberapa situs yang menerapkan *single sign on* tidak menerapkan peringatan untuk melakukan *sign out* pada saat pengguna menekan tombol *sign out* [9].



Gambar 8. Tampilan Peringatan *Log Out* di stackoverflow.com [9]

Kami melakukan percobaan terhadap beberapa aplikasi *web*. Dari 6 perusahaan rintisan Indonesia yang menyandang gelar sebagai *unicorn* [10], empat di antaranya mengimplementasikan *single sign in* Google. Keempat aplikasi *web* tersebut adalah Tokopedia, Traveloka, Bukalapak, dan JD.ID. Keempat situs tersebut tidak memberikan peringatan atas aksi *log out* yang dilakukan pengguna.

D. *Availability*

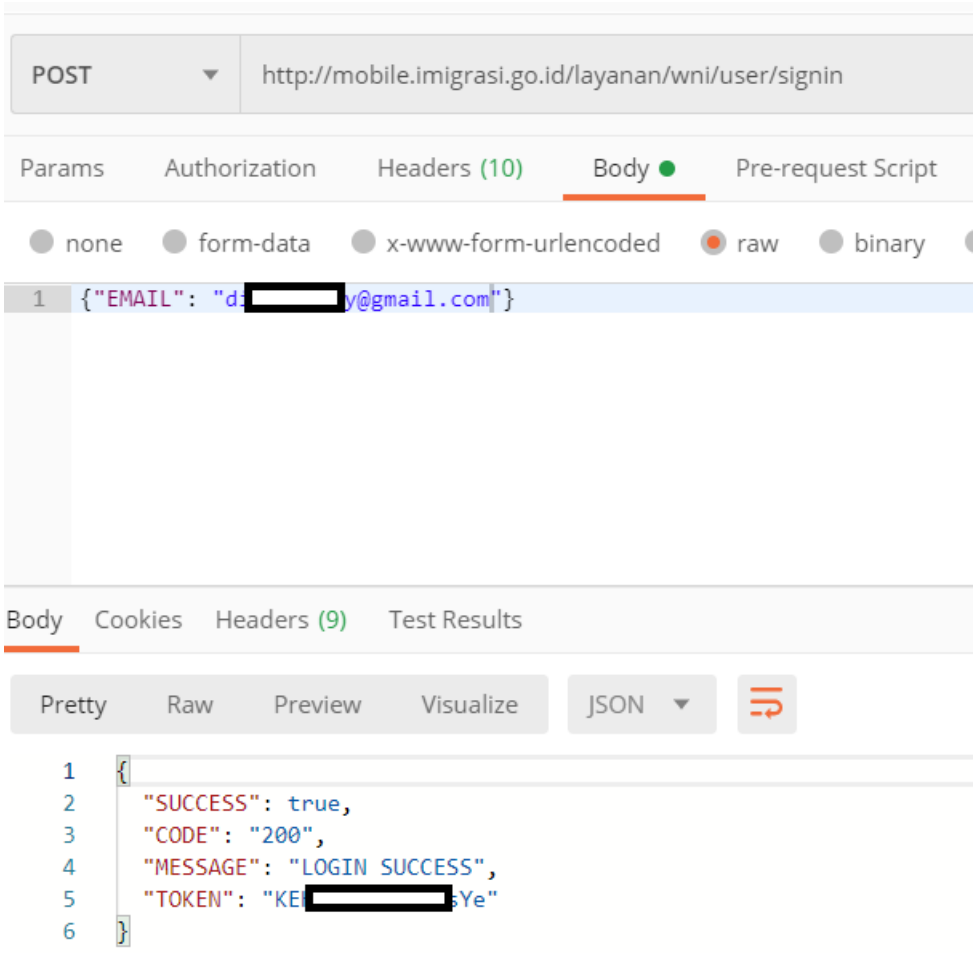
Tidak ada sumber yang cukup untuk menjelaskan mengenai ketersediaan layanan Google. Meskipun demikian, situs Google.com diblokir di sejumlah negara. Google sendiri diblokir di negara Tiongkok [11].

Sejumlah negara yang disanksi embargo oleh Amerika Serikat mungkin memblokir Google [12], namun penulis tidak menemukan referensi yang cukup untuk menyatakan bahwa layanan *single sign on* Google tidak tersedia di negara-negara tersebut.

III. TINJAUAN POTENSI CELAH KEAMANAN

A. Tidak adanya validasi yang cukup

Dalam implementasinya, tidak semua aplikasi *web* mengimplementasikan protokol keamanan *single sign on* yang benar. Dalam pengalaman penulis, terdapat beberapa aplikasi *web* yang dikembangkan dengan tidak semestinya yaitu dengan mengirimkan hanya email pengguna kepada *backend* untuk divalidasi. Padahal seharusnya ID token atau *access token* dikirimkan ke *backend* untuk divalidasi lebih lanjut sebelum menentukan apakah pengguna ini adalah pengguna yang benar.



Gambar 9. Kesalahan Implementasi Google *Sign-in* Terintegrasi di Layanan Aplikasi Paspor

Gambar 9 merupakan salah satu kesalahan implementasi *single sign on* pada aplikasi Layanan Paspor Online yang dikeluarkan oleh Direktorat Jenderal Imigrasi Kemenkumham RI. Penulis telah melaporkan celah keamanan ini kepada *System Analyst* dari pihak terkait pada 19 Juni 2019 dan hingga makalah ini ditulis, belum ada perbaikan yang dilakukan.

Gambar 10. Kesalahan Implementasi Google *Sign-in* Terintegrasi Pada Aplikasi Bonum

Gambar 10 merupakan contoh kesalahan implementasi Google *single sign on* pada aplikasi Bonum (*com.bonum*). *Login* hanya mengirimkan data pengguna tanpa melampirkan *signature* yang diberikan Google.

B. Layanan Google tidak dapat diakses

Menimbang definisi keamanan mencakup ketersediaan layanan, maka pemblokiran layanan Google di negara-negara tertentu membuat pengembang aplikasi *web* perlu mempertimbangkan pengadaan strategi verifikasi identitas alternatif.

IV. KESIMPULAN

Penulis menyimpulkan bahwa Google telah menetapkan standar keamanan yang mencukupi.

Google mempunyai kebijakan berbagi data yang jelas dan diatur dalam kebijakan privasinya. Selain itu meskipun tidak menjelaskan durasi dan isi catatan *log* yang dimilikinya, Google mempunyai catatan *log* aktivitas API dengan durasi 2 minggu menurut informasi Google pada penemuan celah keamanan Google+.

Pengembang aplikasi *web* perlu mendaftarkan aplikasinya terlebih dahulu dan Google akan menentukan tingkat risiko dari aplikasi tersebut. Aplikasi yang memiliki risiko tinggi akan diverifikasi manual.

Setelah itu, pengembang aplikasi *web* dapat mengintegrasikan autentikasi Google pada aplikasi *web* mereka. Pengguna dapat masuk ke Google dan mengaktifkan *2-step verification* untuk lebih mengamankan akun mereka. Fitur *2-step verification* memungkinkan pengguna untuk memverifikasi identitas mereka menggunakan ponsel, kode SMS/telepon, maupun *dongle security key*. Setelah sukses *login* dengan Google, pengguna akan dimintai izin agar Google dapat membagikan data pengguna berupa nama, alamat email, foto profil, dan pilihan bahasa kepada aplikasi *web* tersebut. Apabila aplikasi *web* membutuhkan izin tambahan yang menyangkut data pengguna, Google akan menampilkan sebuah layar permintaan izin tambahan.

Setelah pengguna memberikan izin, Google akan memberikan *access token* OAuth dan ID *token* berformat JWT dengan algoritma RSA-SHA256 untuk diberikan kepada aplikasi *web*. Aplikasi *web* dapat memverifikasi ID *token* yang diberikan menggunakan kunci publik milik Google maupun mengirimkannya ke *endpoint infotoken* yang disediakan Google atau dengan menukarkan *access token* dengan identitas pengguna kepada Google dengan protokol OAuth 2.0 sesuai struktur OpenID.

Di sisi lain, Google tidak menerapkan *single sign off* sehingga pengguna mungkin terkecoh dan berpikir mereka telah keluar dari Google dengan keluar dari aplikasi *web* yang terhubung. Hal ini sebenarnya dapat ditanggulangi dengan mengirimkan peringatan kepada pengguna ketika pengguna berniat keluar dari aplikasi *web* pihak ketiga, namun tidak ada aplikasi *unicorn* Indonesia yang menampilkan pesan ini.

Google sendiri tidak tersedia di sebagian negara, salah satunya Tiongkok. Ini berarti pengguna sebuah aplikasi *web* di negara-negara yang diblokir tidak dapat *login* menggunakan Google. Aplikasi *web* yang menargetkan pengguna di negara-negara terdampak perlu menyiapkan strategi verifikasi identitas lainnya yang tersedia.

Walaupun Google menyediakan sistem yang cukup aman, nyatanya tidak semua aplikasi menerapkan standar keamanan yang telah disediakan. Beberapa aplikasi hanya memberikan memvalidasi alamat email tanpa memvalidasi *signature* atau *access token* yang diberikan, sehingga memungkinkan pengguna untuk menyamar sebagai pengguna lainnya.

ACKNOWLEDGMENT

Penulis ingin mengucapkan terima kasih kepada Bapak Ir. Budi Rahardjo, M.Sc., Ph.D. (Dosen Kelompok Keilmuan Teknik Komputer STEI Institut Teknologi Bandung) atas pengetahuan mengenai keamanan informasi digital dan teknik penulisan makalah.

REFERENCES

[1] Huntington Ventures, “SSO and LDAP Authentication.” [Online]. Tersedia: http://www.authenticationworld.com/Single-Sign-On-Authentication/SSOandLDAP.html. [Diakses 23 Mei 2014]

[2] University of Guelph, “SSO Benefits.” [Online]. Tersedia: https://www.uoguelph.ca/ccs/security/internet/single-sign-sso/benefits. [Diakses 29 April 2020]

[3] Cherdantseva Y. and Hilton J., "Information Security and Information Assurance. The Discussion about the Meaning, Scope and Goals," In: Organizational, Legal, and Technological Dimensions of Information System Administrator. Almeida F., Portela, I. (eds.). IGI Global Publishing, 2013.

[4] Namratha S., “Implementing OAuth.0 using Google Sign-in for a DIY Secure Smart Lock.” [Online]. Tersedia: https://hackernoon.com/implementing-oauth-0-using-google-sign-in-for-a-diy-secure-smart-lock-c918b63900b8. [Diakses 27 Mei 2020]

[5] Google, “OpenID Connect.” [Online]. Tersedia: https://developers.google.com/identity/protocols/oauth2/openid-connect. [Diakses 27 Mei 2020]

[6] Google, “Kebijakan Privasi & Persyaratan.” [Online]. Tersedia: https://policies.google.com/privacy?hl=id-ID. [Diakses 29 Mei 2020]

[7] Google Developers, “Updating developer identity guidelines and registration processes to protect users.” [Online]. Tersedia: https://developers.googleblog.com/2017/05/updating-developer-identity-guidelines.html. [Diakses 31 Mei 2020]

[8] B. Smith, “Project Strobe.” [Online]. Tersedia: https://blog.google/technology/safety-security/project-strobe/. [Diakses 31 Mei 2020]

[9] V. Rastogi and A. Agrawal, "All your Google and Facebook logins are belong to us: A case for single sign-off," *2015 Eighth International Conference on Contemporary Computing (IC3)*, Noida, 2015, pp. 416-421, doi: 10.1109/IC3.2015.7346717.

[10] A. Rizal, “Daftar 6 Startup Unicorn Indonesia Saat Ini.” [Online]. Tersedia: https://infokomputer.grid.id/read/122038532/daftar-6-startup-unicorn-indonesia-saat-ini?page=all. [Diakses 31 Mei 2020]

[11] P. Leskin, “Here are all the major US tech companies blocked behind China’s ‘Great Firewall’.” [Online]. Tersedia: https://www.businessinsider.sg/major-us-tech-companies-blocked-from-operating-in-china-2019-5. [Diakses 31 Mei 2020]

[12] Google. “Countries or regions where G Suite is available.” [Online]. Tersedia: https://support.google.com/a/answer/2891389. [Diakses 31 Mei 2020]

[13] Google. “Turn on 2-Step Verification.” [Online]. Tersedia: https://support.google.com/accounts/answer/185839?hl=en&ref_topic=7189195. [Diakses 1 Juni 2020]