Analisis Keamanan Aplikasi Tanda Tangan Elektronik: Adobe Sign

Edwin Stanic Prasetyo - 18219079
Program Studi Sistem dan Teknologi Informasi
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
E-mail (gmail): 18219079@std.stei.itb.ac.id

***Abstract*— Tanda tangan elektronik(e-*signatures*) merupakan aplikasi kriptografi yang biasa digunakan dalam kehidupan sehari-hari. Penggunaan tanda tangan elektronik menjadi sebuah alternatif yang mudah digunakan dan tetap menjadi sebuah cara yang legal untuk mendapatkan persetujuan pada dokumen elektronik. Pada makalah ini, akan dilakukan analisis terhadap kemanan tanda tangan elektronik yang menjadi fitur pada aplikasi Adobe Sign.**

Keywords—e-signatures; Adobe Sign; Kriptografi; Keamanan

I. PENDAHULUAN

Tanda tangan adalah salah satu identitas yang wajib dimiliki oleh setiap orang untuk keperluan autentikasi. Identitas ini bersifat unik dalam artian berbeda antara satu orang dengan lainnya sehingga bersifat melekat kepada diri seseorang. Tanda tangan pertama kali ditemukan pada orang-orang Sumeria pada tahun 3500 SM dalam bentuk goresan kecil pada tanah liat. Pemanfaatan tersebut terus mengalami perkembangan hingga menciptakan sistem tanda tangan yang lebih kompleks seperti sekarang ini.

Awal mulanya tanda tangan diadopsi oleh masyarakat di seluruh dunia untuk mengautentikasi dokumen cetak. Pembubuhan tanda tangan pada suatu dokumen cetak menandakan bahwa orang tersebut telah membaca dan menyetujui seluruh pernyataan yang ada di dalamnya. Proses autentikasi ini memiliki prosedur yang cukup sederhana dimana seorang pengguna hanya perlu memastikan bahwa setiap butir pernyataan yang tercantum dalam suatu dokumen tidak ada yang janggal dan telah sesuai dengan kesepakatan antara 2 pihak. Apabila dirasa sudah sesuai, penanda tangan hanya perlu mencantumkan identitasnya dalam bentuk guratan yang biasanya terletak pada akhir dokumen. Praktis dan sederhananya tanda tangan membuat metode ini sangat terkenal dan digunakan pada setiap dokumen perjanjian.

Autentikasi dokumen cetak menggunakan tanda tangan memang tidak dapat dipungkiri memiliki banyak kelebihan tetapi tidak berarti tanda tangan tidak memiliki kekurangan. Suatu dokumen yang sudah ditandatangani pada umumnya masih bisa diakses oleh orang lain, khususnya pihak yang bertanggung jawab untuk niat yang jahat. Mereka dapat memodifikasi pernyataan yang terdapat dalam suatu dokumen yang telah dibubuhi tanda tangan dan menyatakan bahwa penanda tangan setuju dengan perjanjian tersebut.

Selain adanya kemungkinan dimodifikasinya suatu dokumen, tanda tangan yang ada juga dapat dipelajari untuk ditiru dan kemudian digunakan pada dokumen lain oleh orang yang tidak bertanggung jawab tersebut. Mereka bertindak seakan-akan menjadi penanda tangan resmi tanpa sepengetahuan pemilik tanda tangan tersebut. Kekurangan-kekurangan dari tanda tangan konvensional ini tentu saja menimbulkan kerugian baik dalam bentuk material maupun non-material. Akan tetapi belum tersedianya metode autentikasi lain dengan tingkat keamanan yang lebih baik namun tetap memenuhi aspek praktis mengakibatkan tanda tangan masih banyak digunakan.

Permasalahan tersebut pada akhirnya memotivasi para ahli di bidang keamanan untuk melakukan inovasi terkait dengan tanda tangan. Hal ini selaras dengan sifat dasar manusia yang tidak pernah puas dan terus belajar dalam menciptakan suatu inovasi yang lebih baik. Perkembangan teknologi dan populernya dunia digital secara tidak langsung juga melahirkan kebutuhan keamanan yang lebih baik lagi. Masyarakat berharap mereka dapat bertukar informasi dan bekerja melalui dunia digital secara aman layaknya beraktivitas pada dunia nyata.

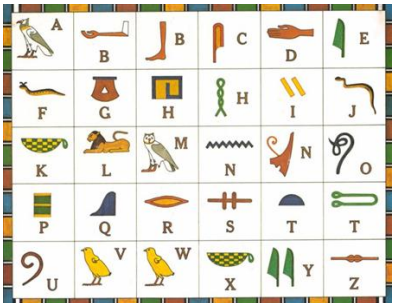
Harapan tersebut menjadi salah satu motivasi yang mendorong para ahli komputer mempelajari tanda tangan lebih dalam lagi untuk mengembangkan suatu sistem tanda tangan di dunia digital. Mereka melakukan sejumlah eksperimen untuk mengadopsi tanda tangan konvensional ke dunia digital dengan sejumlah konfigurasi tambahan. Kerja keras para ahli tersebut pada akhirnya melahirkan tanda tangan elektronik yang banyak digunakan saat ini. Selain tanda tangan elektronik, terdapat juga tanda tangan digital yang memiliki konsep yang cukup berbeda dengan tanda tangan elektronik.

Perkembangan tanda tangan pada akhirnya menambah jenis tanda tangan baru sehingga secara umum ada tiga jenis tanda tangan, yaitu basah/konvensional, elektronik, dan digital. Setiap jenis tanda tangan tersebut banyak dimanfaatkan oleh masyarakat sesuai dengan preferensi masing-masing. Melalui makalah ini, penulis akan menilik keamanan salah satu aplikasi tanda tangan elektronik yaitu Adobe Sign.

II. Dasar Teori

A. Kriptografi

Kriptografi adalah suatu alat yang banyak dimanfaatkan dalam keamanan informasi. Kata kriptografi sendiri berasal dari bahasa Yunani yaitu cryptós yang memiliki arti rahasia dan gráphein yang memiliki arti tulisan. Kriptografi juga dapat didefinisikan sebagai ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, dan autentikasi.



Gambar 1. Hieroglyph (Sumber: https://commons.wikimedia.org/wiki/File:Hieroglyph_picture_write_alphabet.jpg)

Pemanfaatan kriptografi pertama kali ditemukan pada zaman Mesir kuno 4000 tahun yang lalu dimana Bangsa Mesir menggunakan *hieroglyph* yang tidak standard untuk menulis pesan di dinding piramid. Aplikasi kriptografi selanjutnya ditemukan pada zaman Yunani dan Romawi kuno melalui penggunaan alat yang Bernama *scytale*.

Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan. Sifat "aman" sendiri memiliki arti:

1. Terjaga kerahasiaannya (*confidentiality*)
2. Terjaga keasliannya (*data integrity*)
3. Pengirim pesan diyakini adalah pengirim yang asli *(authentication*)
4. Pengirim pesan tidak dapat melakukan penyangkalan (*non-repudiation*) bahwa pihaknya adalah pihak yang mengirim pesan.

Sifat aman yang dimiliki oleh kriptografi inilah yang menyusun layanan-layanan yang dapat disediakan oleh kriptografi antara lain:

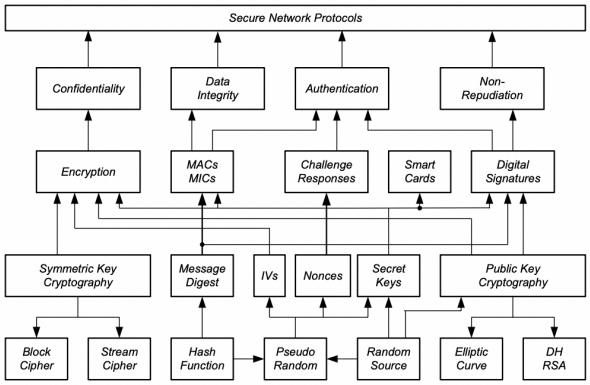
1. Kerahasiaan pesan (*confidentiality/privacy/secrecy*)
2. Keaslian pesan (*data integrity*)
3. Keaslian pengirim dan penerima pesan (*authentication*)
4. Anti penyangkalan (*non-repudiation*)

Salah satu aplikasi dari kriptografi adalah enkripsi, yaitu proses menyandikan plainteks menjadi cipherteks. Pada kehidupan sehari-hari, enkripsi digunakan untuk memproteksi sebuah dokumen yang ada di dalam *storage*, merahasiakan pesan yang dikirim, dan melindungi data-data penting lainnya.

B. Kriptografi Modern

Perkembangan algoritma kriptografi modern diawali dari penggunaan komputer digital untuk keamanan pesan. Komputer digital merepresentasikan data dalam bentuk biner sehingga kriptografi modern beroperasi dalam mode *bit* atau *byte*. Akibatnya, kriptografi modern adalah suatu metode pengamanan informasi yang akan beroperasi dalam mode *bit* atau *byte*.

Secara teknik, algoritma kriptografi modern tetap mengadopsi teknik algoritma kriptografi klasik seperti substitusi dan transposisi. Namun, pada kriptografi modern teknik-teknik tersebut menjadi lebih kompleks supaya sulit untuk dikriptanalisis.



Gambar 2. Diagram Blok Kriptografi Modern (Sumber: https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi-dan-Koding/2021-2022/4%20-%20Kripto-modern-2021.pdf)

Terdapat beberapa kategori cipher berbasis bit antara lain:

1. Cipher Alir (*Stream Cipher*)
   - Beroperasi pada bit tunggal
   - Enkripsi/dekripsi *bit* per *bit*
2. Cipher Blok (*Block Cipher*)
   - Beroperasi pada blok *bit*
   - Enkripsi/dekripsi blok per blok

C. Tanda Tangan

Tanda tangan adalah sebuah identitas berbentuk simbol atau guratan yang diciptakan untuk keperluan autentikasi suatu dokumen perjanjian. Sejarah menceritakan tanda tangan pertama kali ditemukan pada orang Sumerian yang menggunakan tanda tangan dalam bentuk segel. Segel tersebut dibuat dari kumpulan simbol-simbol yang dicetak ke sebuah tanah liat basah. Bentuk tanda tangan terus mengalami perkembangan seiring waktu seperti segel Bernama Hanko yang digunakan oleh orang Jepang pada tahun 57 SM, hingga guratan pada kertas yang mulai banyak digunakan pada tahun 1600.

Identitas ini merupakan suatu bukti kuat yang menunjukkan penanda tangan telah membaca dan menyetujui suatu perjanjian. Keunikan satu tanda tangan dengan tanda tangan lainnya membuat tanda tangan setiap orang bersifat unik sehingga tidak dapat disangkal. Sifat ini menjadi alasan utama mengapa tanda tangan banyak dimanfaatkan dalam perjanjian sebab tidak ada orang lain yang dapat membuat guratan yang sama persis dengan pemilik asli tanda tangan.

Secara umum tanda tangan terbagi menjadi lima jenis, yaitu:

1. *Symbols and Marks*

Gambar 3. Tanda Tangan di Batu pada Zaman Purba (Sumber: https://blog.thegrizzlylabs.com/img/2020-11-20/tablet.png)

Simbol dan tanda-tanda adalah jenis tanda tangan pertama yang banyak digunakan oleh manusia zaman purba. Tanda tangan ini biasanya melibatkan serangakaian simbol yang digabungkan satu sama lain menciptakan suatu kombinasi yang bersifat unik dan menggambarkan ciri khas pemiliknya. Selanjutnya, rangkaian simbol tersebut akan diletakkan pada sebuah media untuk kemudian dicantumkan pada dokumen penting sebagai bentuk autentikasi.

2. *Wet Signatures*

Gambar 4. *Tanda Tangan Konvensional (Sumber: https://www.signaturewrite.com/wp-content/uploads/2020/12/20200728_152020.jpg)*

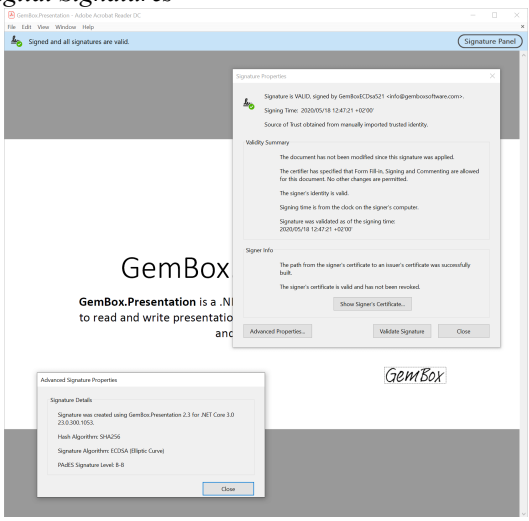
Tanda tangan basah adalah jenis tanda tangan yang paling banyak digunakan oleh manusia di seluruh dunia saat ini. Tanda tangan ini dihasilkan dari guratan-guratan yang membentuk suatu identitas unik. Tanda tangan basah digunakan untuk menandatangani sebuah dokumen fisik sebagai bentuk autentikasi yang dicantumkan dengan tinta.

3. *Electronic Signatures* atau *e-Signatures*

Gambar 5. Tanda Tangan Elektronik (Sumber: https://www.ilovepdf.com/img/blog/sign-with-digital-signature/sign-with-digital-signature.jpg)

Tanda tangan digital merupakan tanda tangan hasil perkembangan tanda tangan konvensional untuk digunakan dalam dunia digital. Jenis tanda tangan ini merupakan representasi digital atau bentuk digitisasi tanda tangan yang biasanya dibuat menggunakan tinta. Layaknya tanda tangan digital, tanda tangan elektronik juga digunakan untuk mengautentikasi sebuah dokumen, tetapi dokumen yang bersifat digital. Saat ini sudah banyak aplikasi yang menyediakan fitur tanda tangan elektronik.

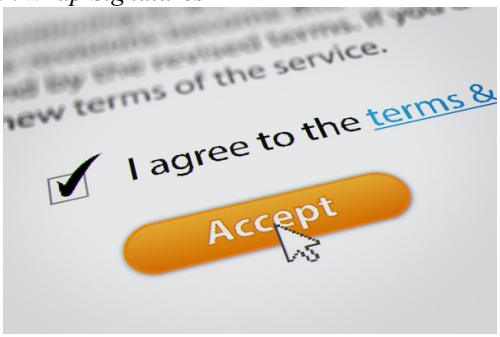
4. *Digital Signatures*



Gambar 6. Tanda Tangan Digital (Sumber: https://www.gemboxsoftware.com/presentation/examples/802/content/PdfDigitalSignature.png)

Tanda tangan digital adalah jenis tanda tangan dalam dunia digital yang cukup berbeda dengan tanda tangan elektronik. Apabila tanda tangan elektronik berfungsi untuk merepresentasikan tanda tangan fisik, tanda tangan digital berfungsi untuk merepresentasikan persetujuan seseorang terhadap suatu dokumen digital. Jenis tanda tangan ini biasanya menggunakan kombinasi fungsi *hash* dan sistem kriptografi kunci-publik yang hasil akhirnya adalah sebuah kode hasil enkripsi tanda tangan.

5. *Click Wrap Signatures*



Gambar 7. Click Wrap Signatures (Sumber: https://blog-test.heylaw.id/wp-content/uploads/2021/10/AdobeStock_286624619_Accept_Click-lower-res-1.jpeg)

Jenis tanda tangan terakhir ini adalah tanda tangan yang biasanya ditemukan pada dunia maya untuk meminta persetujuan pengguna akan suatu hal. Pengguna akan diminta untuk memberikan tanda tangan dengan mencentang sebuah kotak bertuliskan keterangan bahwa pengguna menyetujui suatu kebijakan tertentu.

D. Tanda Tangan Elektronik

Menurut Undang-Undang Republik Indonesia Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, tanda tangan elektronik adalah tanda tangan yang terdiri atas informasi elektronik yang dilekatkan, terasosiasi atau terkait dengan infromasi elektronik lainnya yang digunakan sebagai alat verifikasi atau autentikasi. Sebuah tanda tangan elektronik adalah cara yang legal untuk mendapatkan persetujuan pada dokumen elektronik.

Tanda tangan elektronik memiliki sifat-sifat berikut:

1. Legal
   Sebuah tanda tangan elektronik memiliki kekuatan legal yang mengikat. Terdapat beberapa negara yang memiliki aturan-aturan khusus yang mengatur tentang tanda tangan elektornik
2. Aman
   Tanda tangan elektronik lebih aman daripada tanda tangan tertulis. Dokumen yang sudah ditandatangani akan disimpan dalam lingkungan yang aman dan documen diberikan sertifikat dengan segel yang akan menunjukkan bukti jika sudah diubah
3. Dapat Diaudit
   Terdapat catatan log yang menyimpan sejarah perubahan pada dokumen untuk menujukkan kepatuhan pada aturan yang berlaku.
4. Dapat Diverifikasi
   Proses-proses tanda tangan elektronik menggunakan berbagai macam metode untuk mengautentikasi pengguna. Pada umumnya, proses penandatanganan dilakukan dengan mengirim dokumen yang ingin ditandatangani ke sebuah alamat email yang spesifik. Kemudian, akses penerima dokumen pada akun email dijadikan bentuk autentikasi. Untuk meningkatkan keamanan, dapat dilakukan juga langkah autentikasi tambahan untuk memastikan identitas dari penandatangan.

E. Adobe Sign

Gambar 8. Logo Adobe Sign (Sumber: Google Play Store)

Adobe Sign adalah sebuah fitur dari aplikasi Adobe Acrobat dari perusahaan Adobe. Fitur ini memungkinkan pengguna untuk membubuhkan tanda tangan secara digital sehingga tidak perlu menggunakan kertas dan tinta yang untuk menandatangani sebuah dokumen. Selain menyediakan fitur pembubuhan tanda tangan, pengguna aplikasi juga dapat membuat permintaan tanda tangan kepada orang lain dan melacak status permintaan tersebut.

Adobe Sign hadir sebagai solusi bagi para pengguna yang membutuhkan tanda tangan seseorang secara lebih cepat dan terstruktur. Melalui aplikasi ini, pengguna dapat memberikan tanda tangan dalam bentuk digital tanpa harus terikat dengan keterbatasan ruang dan waktu.

Aplikasi ini dilengkapi dengan berbagai metode autentikasi pengguna dalam memastikan penandatangan adalah pihak resmi yang dimaksud, mulai dari *email*, *password*, *acrobat sign authentication*, nomor telepon, atau nomor identitas kewarganegaraan. Akan tetapi, beberapa metode autentikasi tersebut terbatas untuk paket langganan tertentu.

III. Percobaan

A. Metodologi

Analisis keamanan tanda tangan elektronik dari aplikasi Adobe Sign akan dilakukan dengan membuat permintaan tanda tangan elektronik ke seorang penerima menggunakan berbagai skenario, yaitu:

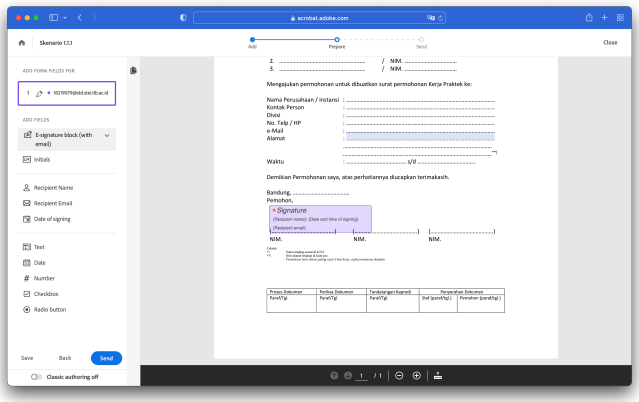
1. Pengujian Autentikasi Penerima dengan *Email*
   1.1 Membuka tautan dari *email* penerima asli
      1.1.1 Menandatangani dokumen dengan akun Adobe yang sama dengan *email* akun penerima
      1.1.2 Menandatangani dokumen dengan akun Adobe yang berbeda dengan *email* akun penerima
      1.1.3 Menandatangani dokumen tanpa menggunakan akun Adobe
   1.2 Membuka tautan yang tersebar
      1.2.1 Menandatangani dokumen dengan akun Adobe yang berbeda dengan *email* akun penerima
      1.2.2 Menandatangani dokumen tanpa menggunakan akun Adobe
2. Pengujian Autentikasi Penerima dengan *Password*
   2.1 Membuka tautan dari *email* penerima asli

2.1.1 Menandatangani dokumen dengan memasukkan *password* yang benar
2.1.2 Menandatangani dokumen dengan memasukkan *password* yang salah

2.2 Membuka tautan yang tersebar
2.2.1 Menandatangani dokumen dengan memasukkan *password* yang benar
2.2.2 Menandatangani dokumen dengan memasukkan *password* yang salah

Pengujian permintaan tanda tangan elektronik dengan metode autentikasi pengguna menggunakan *email* bertujuan untuk mendeteksi apakah Adobe berhasil melacak *email* penandatangan. Selanjutnya akan dianalisis apakah akses hanya diberikan kepada *email* penadantangan yang resmi atau diberikan juga kepada *email* yang tidak dikenali.

Adapun pengujian permintaan tanda tangan elektronik dengan metode autentikasi penerima menggunakan *password* bertujuan untuk mengetahui apakah dokumen bisa dibuka apabila *password* tidak diketahui.



Gambar 9. Permintaan Tanda Tangan pada Dokumen

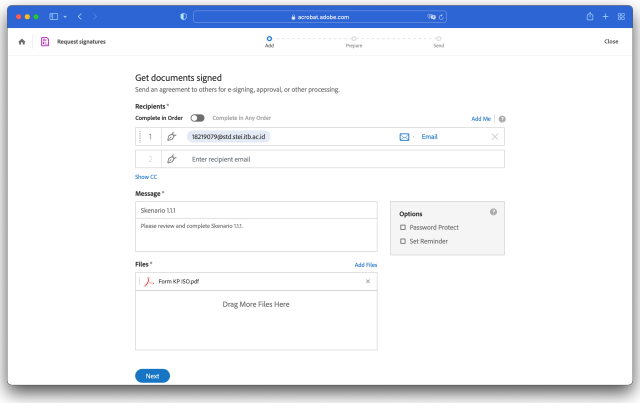
Semua skenario akan dilakukan dengan permintaan pengisian satu kolom saja, yaitu tanda tangan pada kolom tanda tangan yang terdapat dalam dokumen.

B. Hasil Percobaan

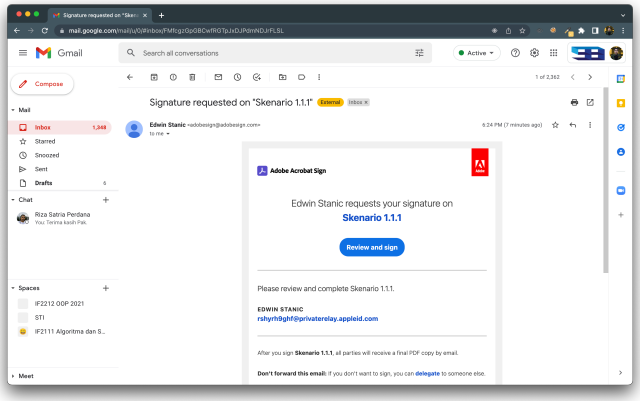
Berikut ini adalah hasil dari eksperimen dari skenario-skenario yang telah dituliskan pada bagian A:

1. Skenario 1.1.1

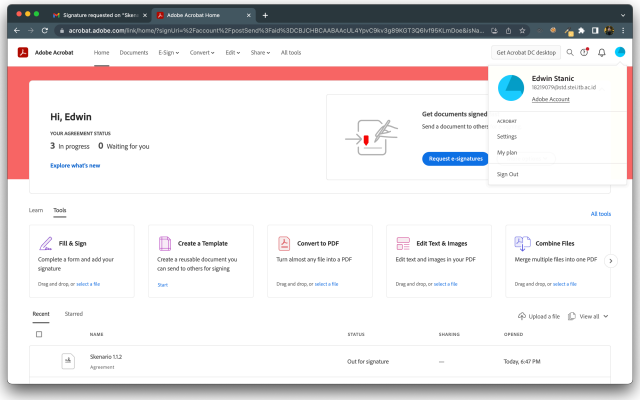
Email Penerima : 18219079@std.stei.itb.ac.id
Email Akun Adobe : 18219079@std.stei.itb.ac.id



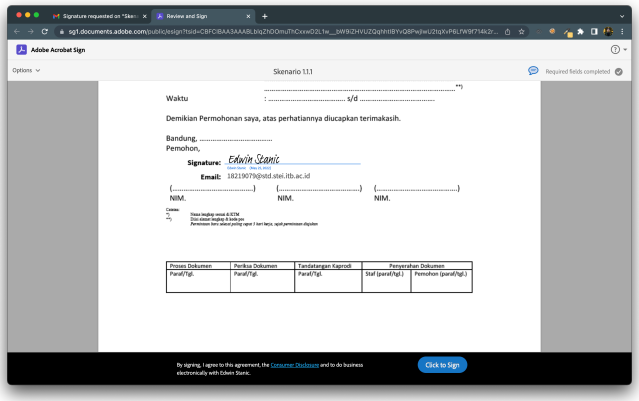
Gambar 10. Pengiriman Permintaan Tanda Tangan ke Email Penerima



Gambar 11. Penerimaan Email oleh Penerima



Gambar X. Akses Adobe menggunakan Akun dengan Email yang Sama dengan Email Penerima



Gambar 12. Penandatanganan Dokumen dengan Akun Adobe Penerima yang Sesuai

Skenario 1.1.1

Final Audit Report 2022-05-25

Created:	2022-05-25
By:	Edwin Stanic (rshyrh9ghf@privaterelay.appleid.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAAIfCx939mvc-obokN_eo7tziPWwtkl367

"Skenario 1.1.1" History

Document created by Edwin Stanic (rshyrh9ghf@privaterelay.appleid.com)
2022-05-25 - 11:29:45 AM GMT

Document emailed to Edwin Stanic (18219079@std.stei.itb.ac.id) for signature
2022-05-25 - 11:34:20 AM GMT

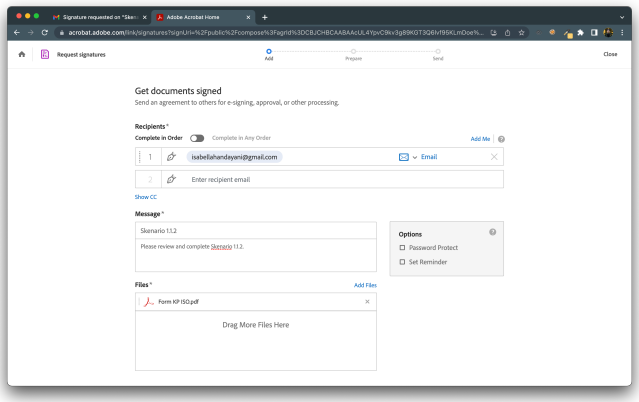
Email viewed by Edwin Stanic (18219079@std.stei.itb.ac.id)
2022-05-25 - 11:34:57 AM GMT

Document e-signed by Edwin Stanic (18219079@std.stei.itb.ac.id)
Signature Date: 2022-05-25 - 11:35:18 AM GMT - Time Source: server

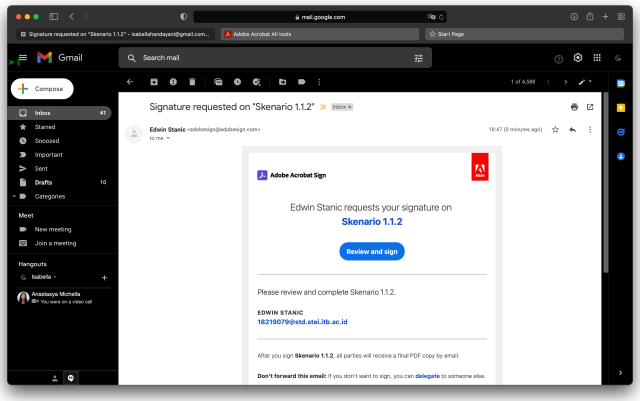
Agreement completed.
2022-05-25 - 11:35:18 AM GMT

Gambar 13. Bukti Audit Skenario 1.1.1

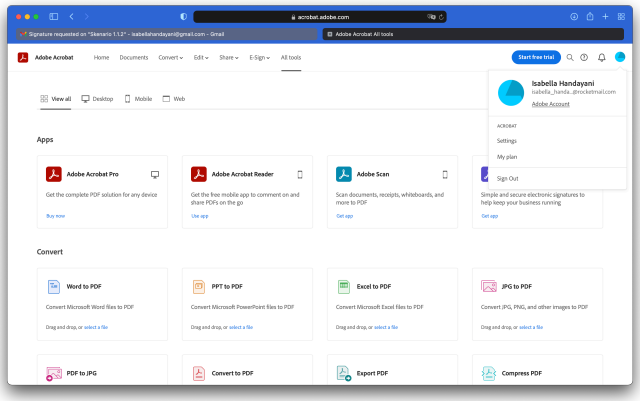
2. Skenario 1.1.2
Email Penerima : isabellahandayani@gmail.com
Email Akun Adobe : isabella_handayani@rocketmail.com



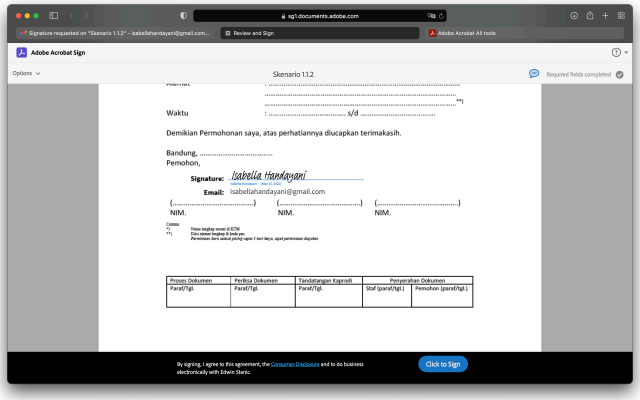
Gambar 14. Pengiriman Permintaan Tanda Tangan ke Email Penerima



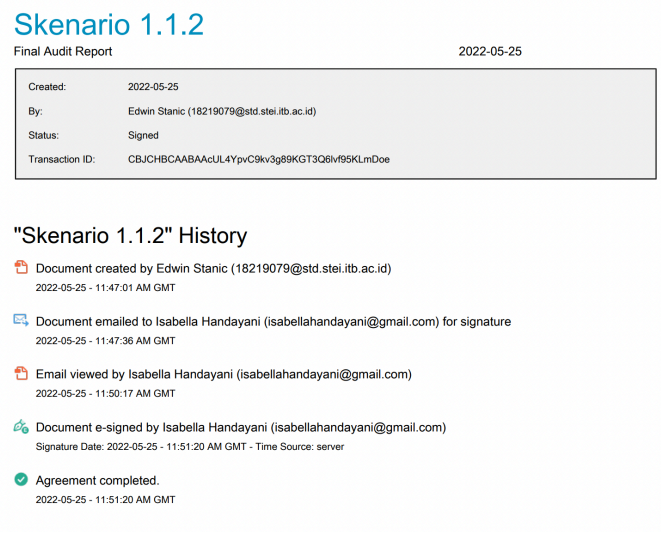
Gambar 15. Penerimaan Email oleh Penerima



Gambar 16. Akses Adobe menggunakan Akun dengan Email yang Berbeda dengan Email Penerima

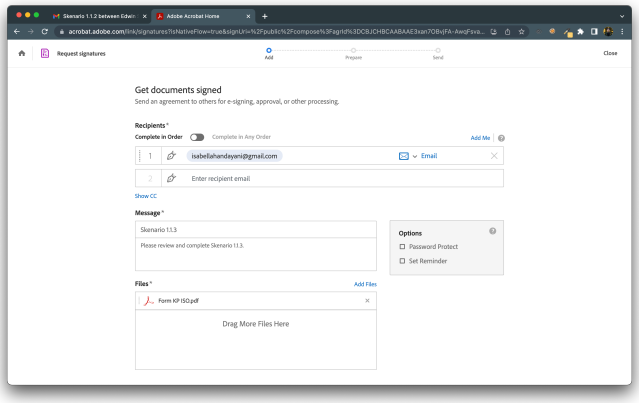


Gambar 17. Penandatanganan Dokumen dengan Akun Adobe Penerima yang Berbeda

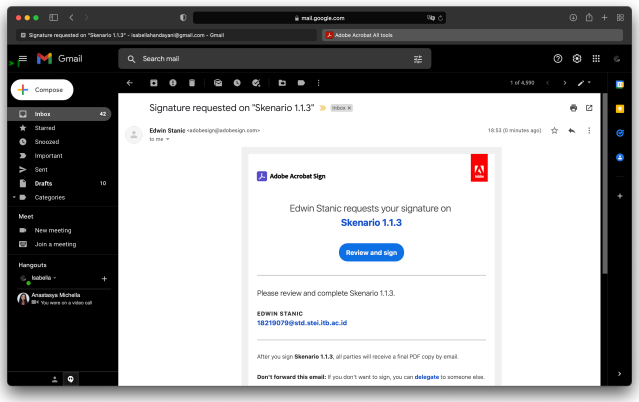


Gambar 18. Bukti Audit Skenario 1.1.1

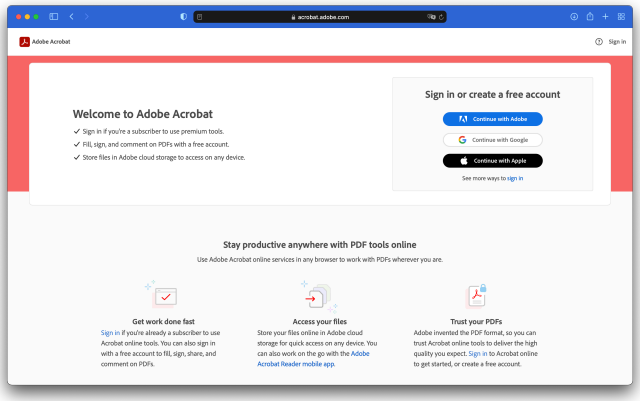
3. Skenario 1.1.3
Email Penerima : isabellahandayani@gmail.com
Email Akun Adobe : -



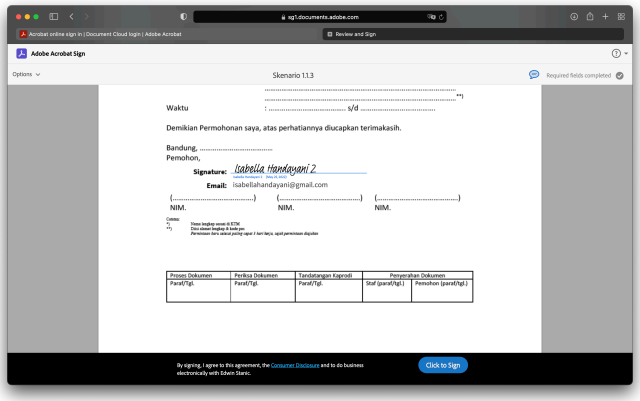
Gambar 19. Pengiriman Permintaan Tanda Tangan ke Email Penerima



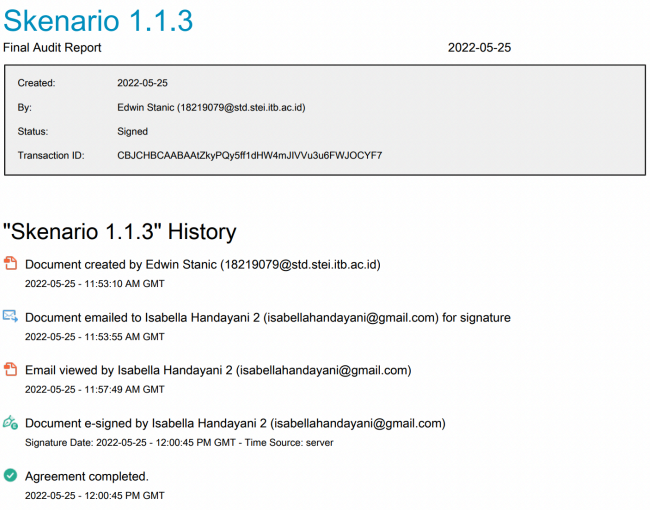
Gambar 20. Penerimaan Email oleh Pengguna



Gambar 21. Akses Adobe Tanpa Menggunakan Akun

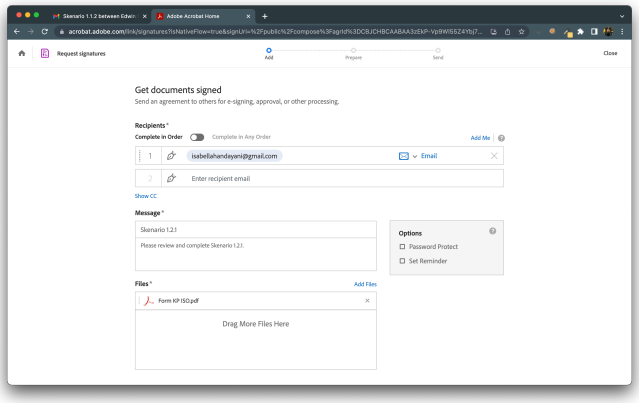


Gambar 22. Penandatanganan Dokumen Tanpa Menggunakan Akun Adobe

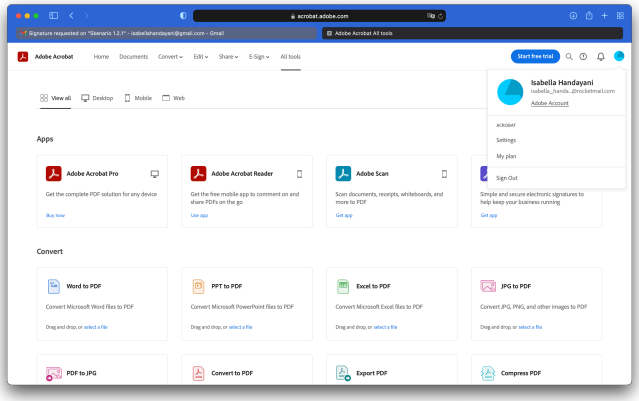


Gambar 23. Bukti Audit Skenario 1.1.3

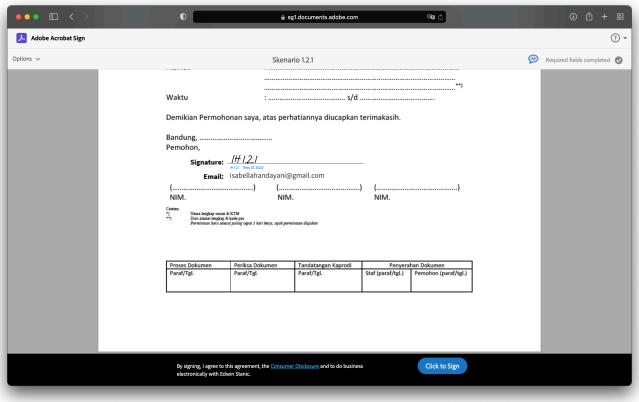
4. Skenario 1.2.1
Email Penerima : isabellahandayani@gmail.com
Email Akun Adobe : isabella_handayani@rocketmail.com



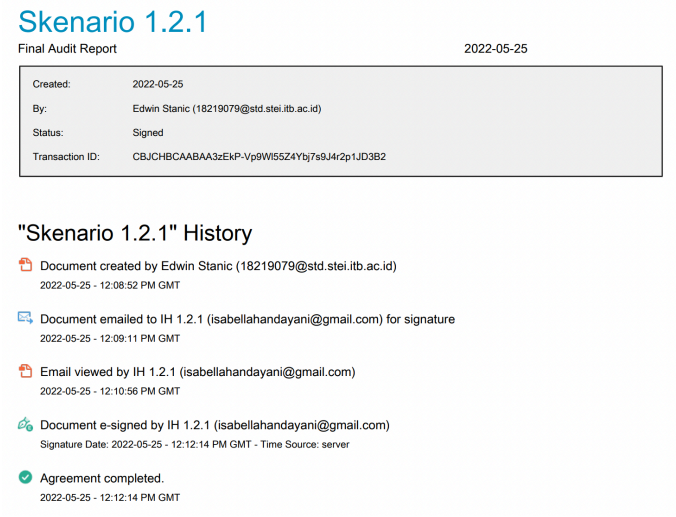
Gambar 24. Pengiriman Permintaan Tanda Tangan ke Email Penerima



Gambar 25. Akses Adobe menggunakan Akun dengan Email yang Berbeda dengan Email Penerima



Gambar 26. Penandatanganan Dokumen dengan Akun Adobe Penerima yang Berbeda

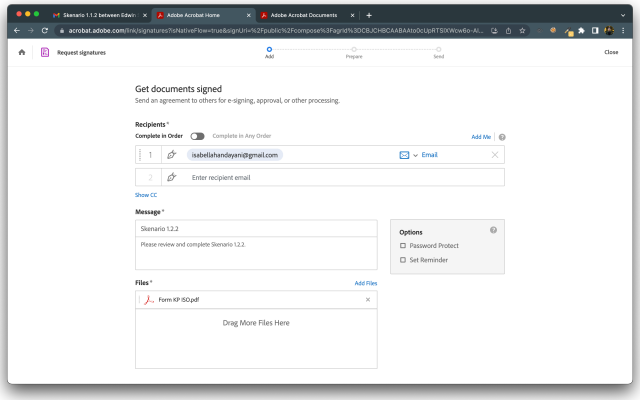


Gambar 27. Bukti Audit Skenario 1.2.1

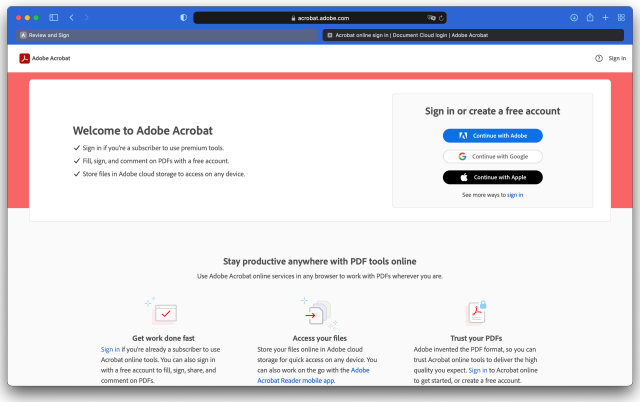
5. Skenario 1.2.2

Email Penerima : isabellahandayani@gmail.com

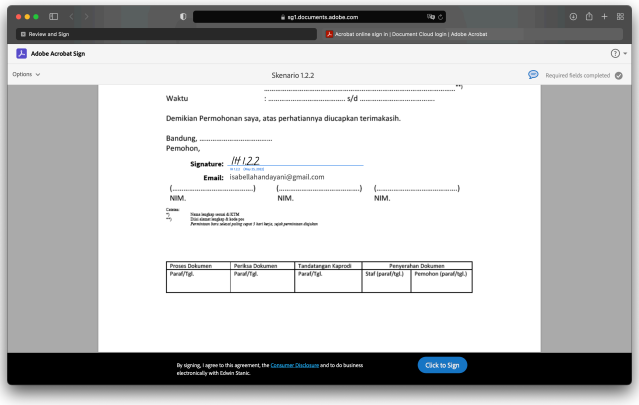
Email Akun Adobe : -



Gambar 28. Pengiriman Permintaan Tanda Tangan ke Email Penerima



Gambar 29. Akses Adobe Tanpa Menggunakan Akun



Gambar 30. Penandatanganan Dokumen Tanpa Menggunakan Akun Adobe

Skenario 1.2.2

Final Audit Report 2022-05-25

Created:	2022-05-25
By:	Edwin Stanic (18219079@std.stei.itb.ac.id)
Status:	Signed
Transaction ID:	CBJCHBCAABAAto0cUpRTSlXWcw6o-AIJfbdok3fqfo7k

"Skenario 1.2.2" History

Document created by Edwin Stanic (18219079@std.stei.itb.ac.id)
2022-05-25 - 12:16:57 PM GMT

Document emailed to IH 1.2.2 (isabellahandayani@gmail.com) for signature
2022-05-25 - 12:17:18 PM GMT

Email viewed by IH 1.2.2 (isabellahandayani@gmail.com)
2022-05-25 - 12:17:27 PM GMT

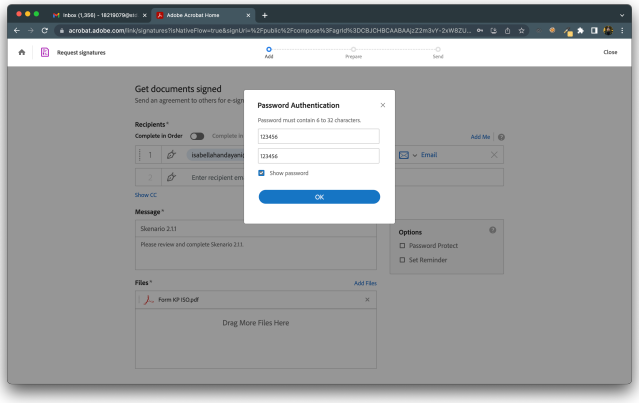
Document e-signed by IH 1.2.2 (isabellahandayani@gmail.com)
Signature Date: 2022-05-25 - 12:19:08 PM GMT - Time Source: server

Agreement completed.
2022-05-25 - 12:19:08 PM GMT

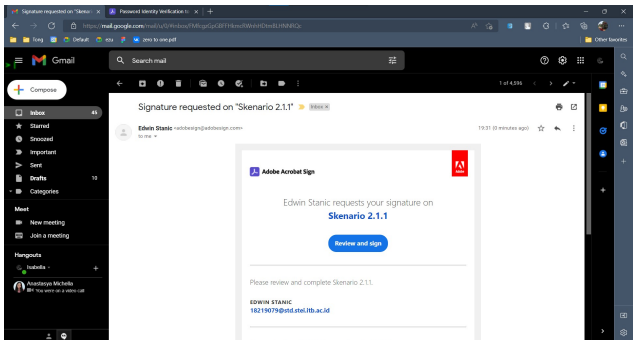
Gambar 31. Bukti Audit Skenario 1.2.1

6. Skenario 2.1.1

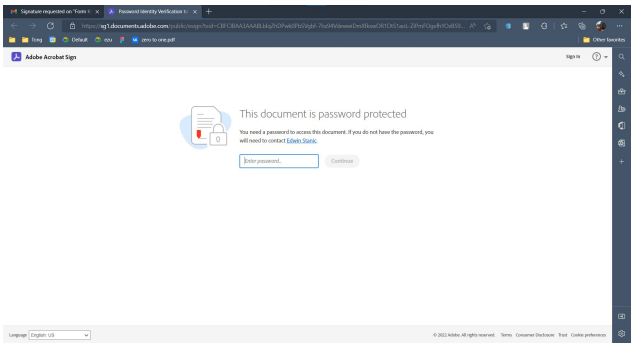
Email Pengguna : isabellahandayani@gmail.com
Password : 123456



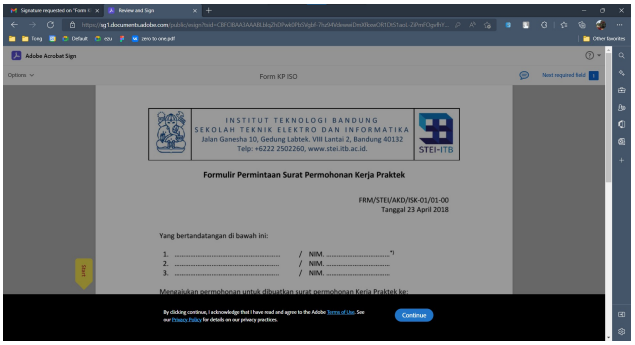
Gambar 32. Pengiriman Permintaan Tanda Tangan ke Email Penerima



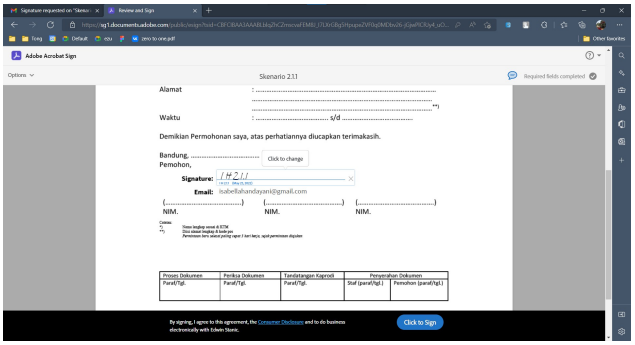
Gambar 33. Penerimaan Email oleh Pengguna



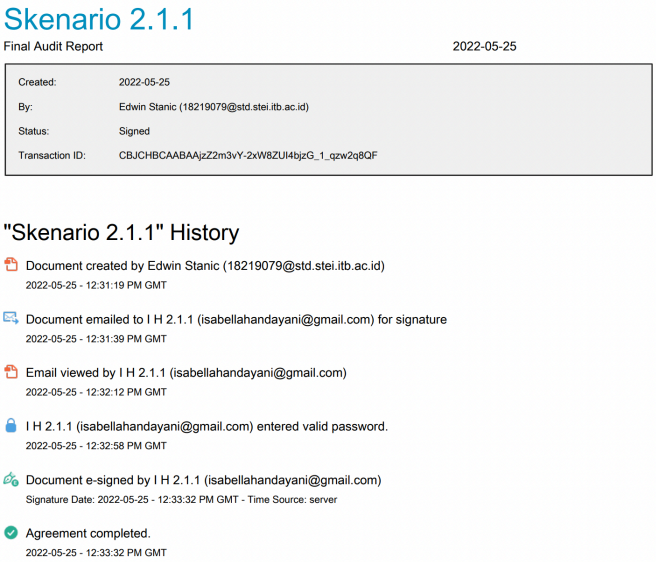
Gambar 34. Permintaan Password oleh Adobe



Gambar 35. Tampilan Setelah Memasukkan Password yang Benar



Gambar 36. Penandatanganan Dokumen dengan Password yang Benar

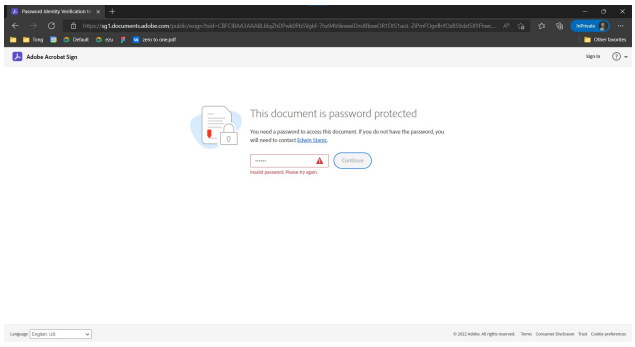


Gambar 37. Bukti Audit Skenario 2.1.1

7. Skenario 2.1.2

Email Pengguna : isabellahandayani@gmail.com
Password : 123456

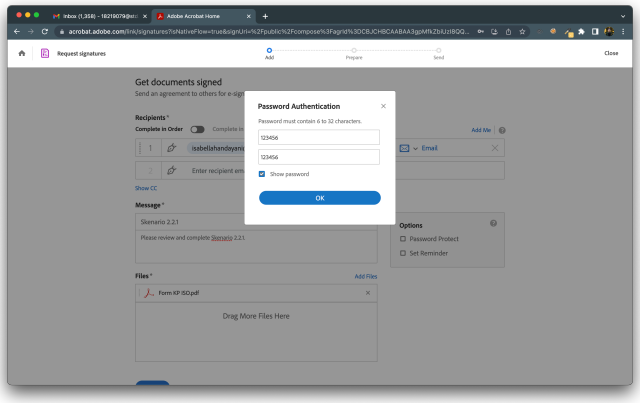
Percobaan skenario 2.1.2 dilaksanakan dengan langkah-langkah yang sama seperti skenario 2.1.1 mulai dari gambar 32 – gambar 34 yang dilanjutkan dengan langkah seperti lampiran *screenshot* berikut.



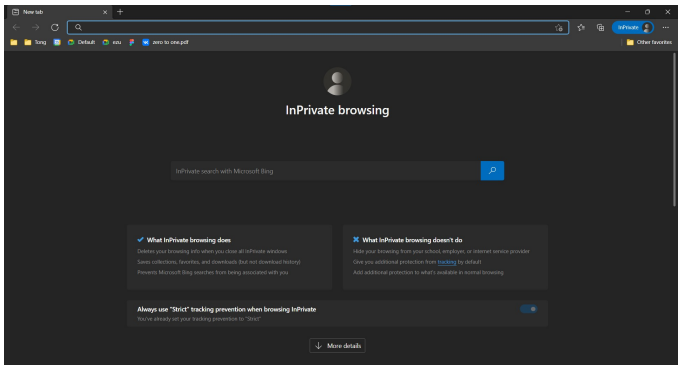
Gambar 38. Tampilan Ketika Memasukkan Password yang Salah

8. Skenario 2.2.1

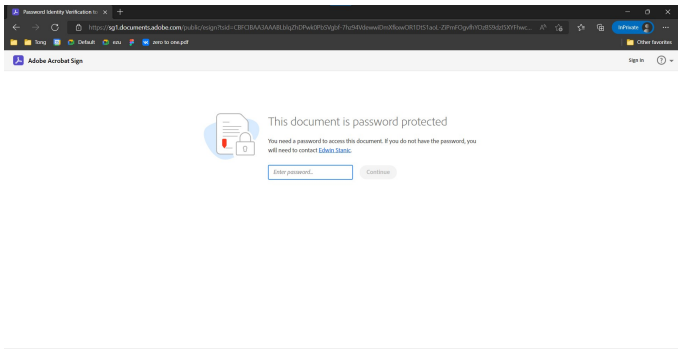
Email Pengguna : isabellahandayani@gmail.com
Password : 123456



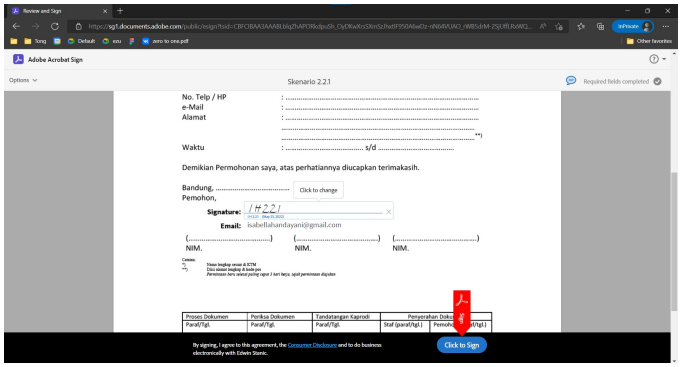
Gambar 39. Pengiriman Permintaan Tanda Tangan ke Email Penerima



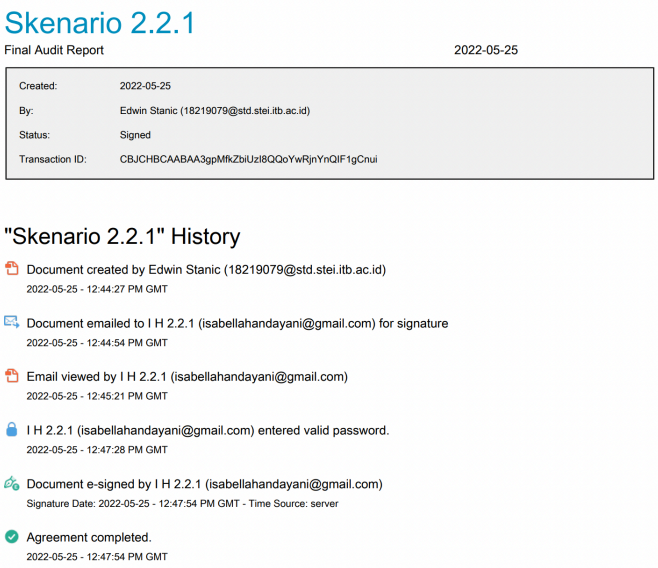
Gambar 40. Pembukaan Tab Incognito



Gambar 41. Permintaan Password oleh Adobe



Gambar 42. Penandatanganan Dokumen dengan Password yang Benar

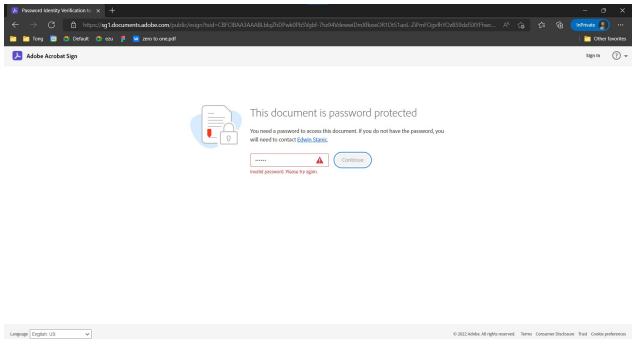


Gambar 43. Bukti Audit Skenario 2.2.1

9. Skenario 2.2.2

Email Pengguna : isabellahandayani@gmail.com
Password : 123456

Percobaan skenario 2.2.1 dilaksanakan dengan langkah-langkah yang sama seperti skenario 2.1.1 mulai dari gambar 39 – gambar 41 yang dilanjutkan dengan langkah seperti lampiran *screenshot* berikut.



Gambar 44. Tampilan Ketika Memasukkan Password yang Salah

IV. Analisis dan Pembahasan

Berdasarkan pelaksanaan percobaan yang terbagi menjadi beberapa skenario, diketahui bahwa Adobe tidak melakukan pemeriksaan *email* penerima yang akan menandatangani dokumen. Pada percobaan skenario 1.1.1-1.1.3 yaitu pengujian autentikasi penerima dengan *email* diketahui bahwa pengaksesan dokumen dapat dilakukan baik dengan akun Adobe yang sesuai, akun Adobe yang berbeda, maupun tidak menggunakan akun Adobe sama sekali. Hal ini menunjukkan bahwa Adobe tidak melakukan autentikasi penanda tangan ketika akan membubuhkan tanda tangan pada dokumen terkait. Autentikasi hanya dilakukan di awal melalui *email* penerima sehingga hanya penerima resmi yang dapat mengakses dan mendantangani dokumen.

Selanjutnya pada skenario percobaan 1.2.1-1.2.3 ditunjukkan kemungkinan *email* penerima dibajak atau tautan untuk menandatangani dokumen tersebar tanpa diketahui oleh penerima. Percobaan ini dilakukan dengan menggunakan *tab incognito* dan mengakses dokumen dengan tautan yang telah disalin dari *email* penerima. Berdasarkan percobaan, diketahui bahwa pengaksesan dokumen masih berhasil dilakukan tanpa adanya pemeriksaan lebih lanjut. Kekurangan ini menunjukkan bahwa autentikasi Adobe yang hanya dilakukan sekali pada pengiriman *email* di awal tidak dapat mengatasi kemungkinan adanya penyerangan atau pencurian tautan dari *email* yang telah dibajak. Akibatnya, mungkin saja suatu dokumen ditandatangani oleh pihak lain yang tidak bertanggung jawab tanpa sepengetahuan penerima asli dan menimbulkan kerugian material atau non-material. Penerima resmi *email* dibuat seakan-akan menyetujui setiap butir pernyataan yang ada dalam dokumen tersebut. Hal ini tentu saja adalah kesalahan yang fatal karena Adobe tidak dapat memastikan keaslian pihak penanda tangan setelah mengirimkan *email* pengguna.

Setelah melakukan pengujian autentikasi penerima dengan *email* pada skenario 1.1 dan skenario 1.2, selanjutnya dilakukan juga pengujian autentikasi penerima dengan *password* melalui skenario 2.1 dan 2.2. Hasil percobaan skenario ini menunjukkan bahwa dokumen hanya dapat diakses apabila orang yang mengakses dokumen mengetahui *password* yang telah dikonfigurasikan untuk dokumen tersebut. Permintaan tanda tangan menggunakan metode autentikasi *password* memiliki lapisan pertahanan tambahan sebagaimana penerima akan diminta untuk memasukkan *password* ketika hendak membuka dokumen.

Celah keamanan khususnya pada metode autentikasi *email* dapat terjadi karena Adobe menggunakan asumsi perilaku pengguna yang salah. Mereka mengasumsikan bahwa setiap pengaksesan dokumen akan dilakukan oleh pengguna yang resmi. Peristiwa ini terjadi ketika mencoba mengakses dokumen menggunakan akun Adobe yang berbeda atau melalui tautan yang berbeda. Setiap penandatanganan akan dikenal sebagai aksi dari penerima asli. Asumsi yang salah tersebut seharusnya tidak diadopsi dalam pengembangan sistem mengingat akan selalu ada pihak yang memanfaatkan celah keamanan tersebut. Akibatnya, terdapat risiko pengaksesan dokumen yang ilegal dan tidak diketahui karena tidak adanya catatan pengaksesan dokumen.

Setiap pihak yang memiliki tautan dari dokumen terkait dapat mengakses dokumen dan menandatanganinya. Berdasarkan hal tersebut, dapat dikatakan tingkat keamanan aplikasi Adobe Sign tidak cukup baik dan melanggar kode etik Association of Computing Machinery (ACM) 1.04 yang menyatakan bahwa suatu perangkat lunak harus menginformasikan potensi risiko yang dialami pengguna ketika menggunakan perangkat lunak terkait. Namun, masalah keamanan yang ditemukan pada autentikasi pengguna dengan *email* dapat diatasi apabila metode autentikasi yang digunakan adalah *password*.

V. Kesimpulan

Adobe Sign adalah aplikasi penyedia tanda tangan elektronik yang memiliki celah keamanan pada salah satu metode

autentikasinya. Hal ini ditunjukkan melalui percobaan dan diketahui bahwa dokumen dapat diakses tanpa menggunakan akun Adobe yang sesuai dan menggunakan tautan yang mungkin tersebar tanpa diketahui oleh penerima sama sekali. Celah keamanan tersebut terjadi akibat adanya kesalahan asumsi perilaku pengguna yang berujung tidak adanya lapisan pertahanan tambahan untuk mengautentikasi orang ketika membuka suatu dokumen. Akan tetapi, kekurangan ini dapat diatasi apabila pengguna memilih metode autentikasi *password* yang akan memaksa orang memasukkan *password* ketika membuka dokumen terkait.

UCAPAN TERIMA KASIH

Penulis ingin memanjatkan rasa syukur kepada Tuhan Yang Maha Esa atas rahmat penyertaan-Nya sehingga makalah ini dapat diselesaikan. Penulis juga ingin mengucapkan terima kasih yang sebesar-besarnya atas pengajaran yang diberikan oleh Dr. Ir. Rinaldi Munir, M.T. selaku dosen mata kuliah II4031 Kriptografi dan Koding STI.

REFERENSI

[1] Munir, R. "Pengantar Kriptografi STI". https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi-dan-Koding/2021-2022/1%20-%20Pengantar-Kriptografi-STI-(2021).pdf. Diakses tanggal 25 Mei 2022 11.35 WIB.

[2] Munir, R. "Kriptografi Modern". https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi-dan-Koding/2021-2022/4%20-%20Kripto-modern-2021.pdf. Diakses tanggal 25 Mei 2022 11.50 WIB.

[3] Munir, R. "Tanda Tangan Digital". https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi-dan-Koding/2021-2022/21%20-%20Tanda-tangan-digital-2021.pdf. Diakses tanggal 25 Mei 2022 12.23 WIB.

[4] Ndukwu, D. "5 types of signatures and when to use them". https://usefulpdf.com/blog/types-of-signatures/. Diakses tanggal 25 Mei 2022 12.47 WIB.

[5] DocuSign Contributor. "From the Quill to the Stylus: The History of the Signature in Celebration of National ESIGN Day". https://www.docusign.com/blog/quill-stylus-history-signature-celebration-national-esign-day#:~:text=The%20Sumerians%20invented%20the%20earliest,be%20pressed%20into%20wet%20clay.&text=Japan%20began%20to%20use%20Hanko,to%20denote%20authorship%20and%20ownership. Diakses tanggal 25 Mei 2022 13.03 WIB.

[6] Adobe. "Adobe Acrobat Sign FAQ". https://helpx.adobe.com/sign/faq.html. Diakses tanggal 25 Mei 2022 13.37 WIB.

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 25 Mei 2022

Edwin Stanic Prasetyo
18219079