13

IDENTITAS DIGITAL

(Digital Identity)

Model identitas digital, prinsip privasi, dan teknologi ID

Token berbasis kriptografi untuk verifikasi identitas yang aman

Disiapkan oleh Ahmad Subagyo

Sumber materi: American Academy, 2021

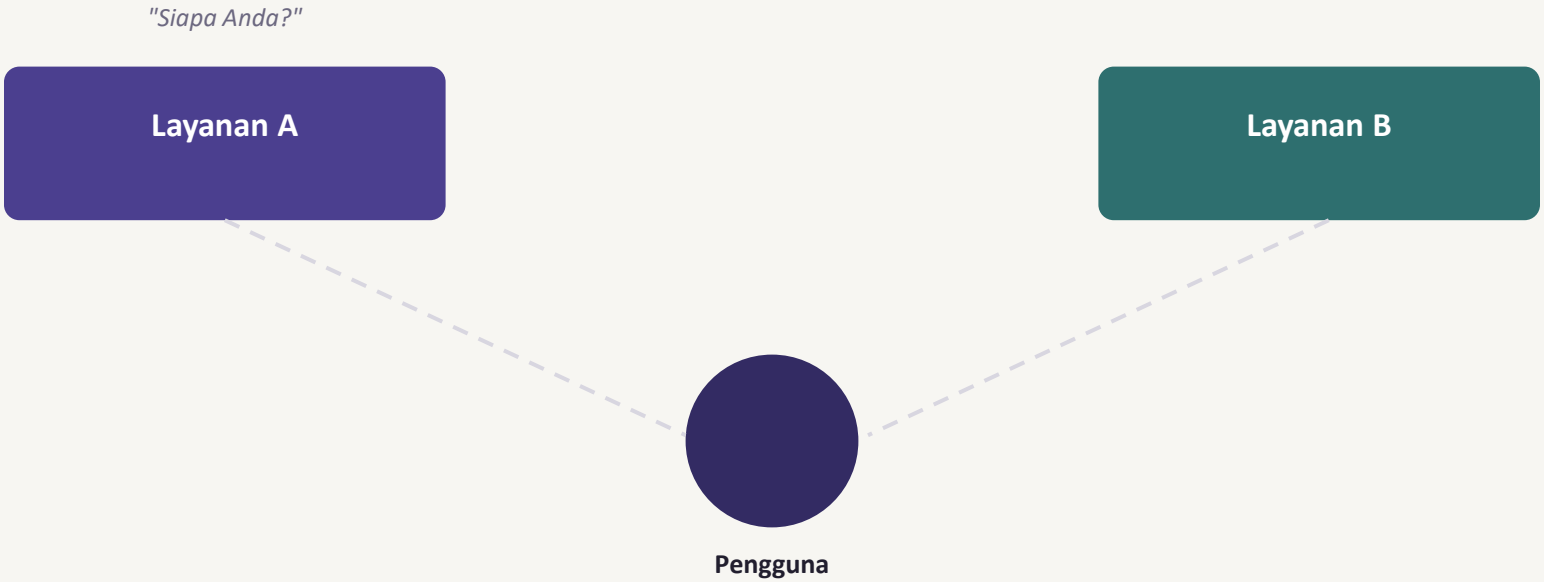
BAGIAN 1

Model-Model Identitas Digital

MODEL IDENTITAS

Silo Identitas (Identity Silos)

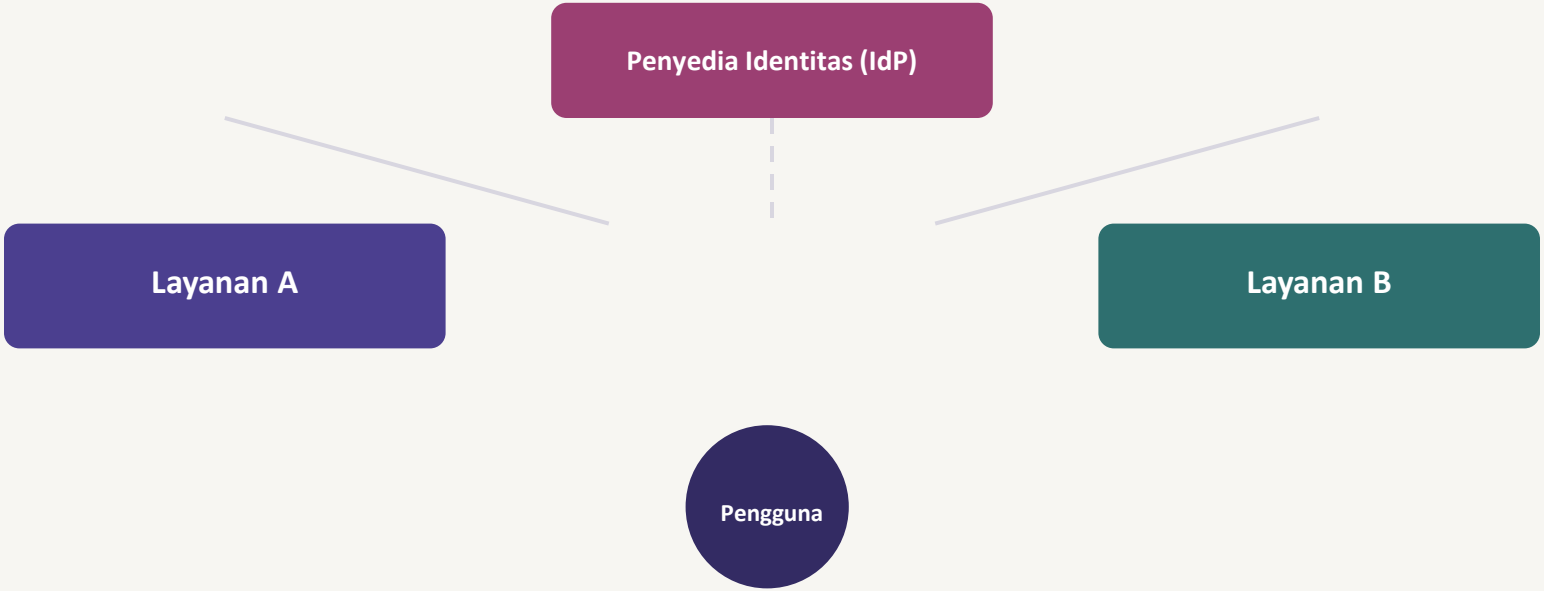
Setiap layanan menyimpan dan memverifikasi identitas penggunanya secara terpisah — pengguna harus membuktikan identitasnya berulang kali pada setiap layanan yang berbeda, tanpa ada berbagi data antar-sistem.



Kredensial terpisah, tidak saling mengenal satu sama lain — pengguna harus login ulang di setiap layanan.

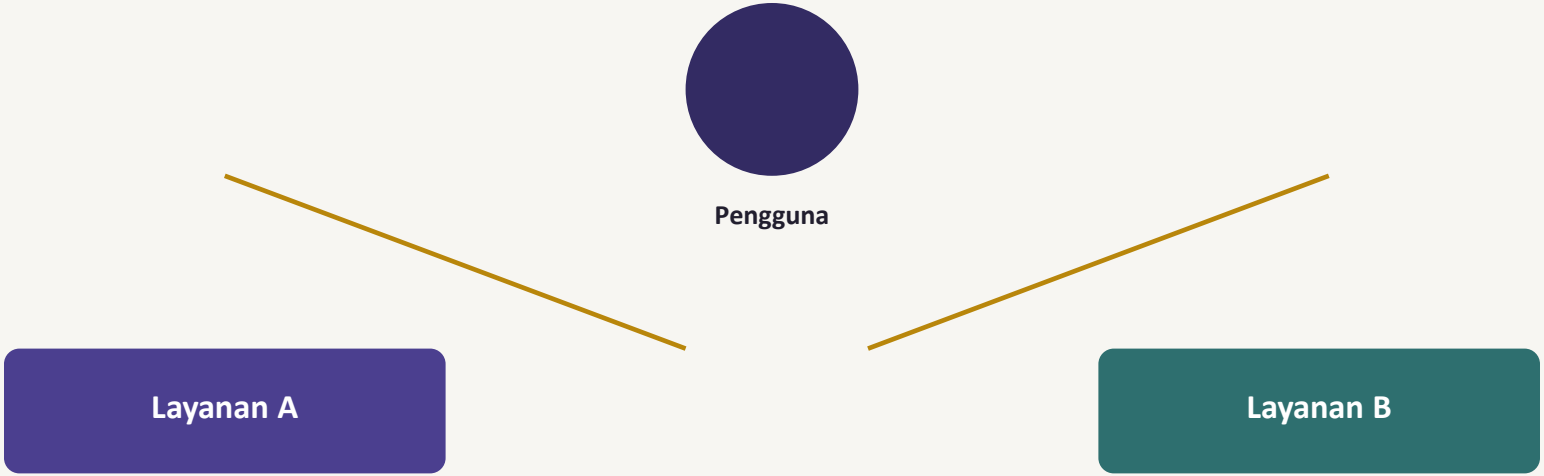
Identitas Terfederasi (Federated Identity)

Sejumlah layanan sepakat mempercayai satu penyedia identitas (Identity Provider) yang sama, sehingga pengguna dapat masuk ke berbagai layanan menggunakan satu kredensial yang sama.



Identitas Berpusat pada Pengguna (User-Centric)

Pengguna sendiri yang mengontrol identitas digitalnya dan memutuskan atribut mana yang dibagikan ke layanan mana — tanpa bergantung sepenuhnya pada satu penyedia identitas pusat.



Pengguna memilih sendiri atribut apa yang dibagikan pada tiap layanan

Upaya Pengembangan Identitas Berpusat pada Pengguna

- Microsoft CardSpace (sebelumnya bernama InfoCard) — komponen UI dan layanan untuk mengelola "kartu" identitas yang diterbitkan sendiri (self-issued) maupun dikelola pihak lain.
- Liberty Alliance iClient/TMa (Intel, NTT, dan lainnya) — memperluas protokol Liberty Alliance ID-WSF.
- Higgins Project (IBM, Novell, dan pemain kecil lainnya) — mencakup OSIS (identity selector yang kompatibel dengan CardSpace), OpenID (autentikasi berbasis URL untuk blogging, bukan berfokus keamanan), Bandit (Novell), dan Heraldry Identity Project (Apache Software Foundation).

PRINSIP

"Hukum" Identitas (Microsoft & IPC Ontario)

Kontrol dan Persetujuan Pengguna

Pengguna dapat menyimpan data identitasnya sendiri dan mengendalikan pengungkapannya.

Pengungkapan Minimal untuk Penggunaan Terbatas

Membatasi cakupan penggunaan sekunder yang tidak sah.

Pihak yang Dapat Dijustifikasi

Keterlibatan suatu pihak dalam relasi identitas harus dapat dijustifikasi.

Identitas Terarah (Directed Identity)

Identifier satu arah (unidirectional) untuk meminimalkan keterkaitan (linkage) antar-situs.

Pluralisme Operator dan Teknologi

Mendukung beragam operator dan teknologi identitas.

Integrasi Manusia & Pengalaman Konsisten

Pengalaman pengguna yang konsisten di berbagai konteks.

Berpusat pada Pengguna: Berkah atau Ancaman bagi Privasi?

Menjadikan pengguna sebagai "titik kendali" (choke point) saja TIDAK CUKUP untuk melindungi privasi.

- Skenario terburuk: pengguna justru MEMPERLUAS berbagi data identitas lintas domain secara luas.
- Setiap transfer data yang berpusat pada pengguna dapat menciptakan identifier/handle lintas domain yang sama — setelah itu, organisasi dapat saling bertukar data pengguna tanpa keterlibatan pengguna, dan pencuri identitas dapat dengan mudah menembus apa yang dulunya "silo" identitas terpisah.
- CardSpace adalah ENABLER bagi Privacy Enhancing Technologies (PETs), bukan PET itu sendiri. Versi saat ini belum sepenuhnya mematuhi "hukum" identitas dan HARUS digunakan bersama PETs.

Karakteristik yang Mendukung Privasi

Pertanyaan kunci: dapatkah subjek data (data subject)...

- Memilih sendiri Identity Provider (IdP) yang sesuai dengan kebutuhan Relying Party (RP)?
- Memberikan (dan menahan) persetujuan atas pengungkapan data?
- Menyembunyikan identitas RP dari IdP, dan permintaan RP dari IdP?
- Melihat data identitas yang sebenarnya, atau apakah data terenkripsi untuk Service Provider (SP)?
- Mengungkapkan data atribut pada kredensial identitas secara selektif (selective disclosure)?
- Menyimpan dan mengelola kredensial identitas jangka panjang secara lokal?
- Menghindari correlation handle antar-IdP dan SP — atau justru (tanpa disadari) menautkan seluruh relasi akun pada setiap pengungkapan?

BAGIAN 2

ID Token Berbasis Kriptografi (U-Prove)

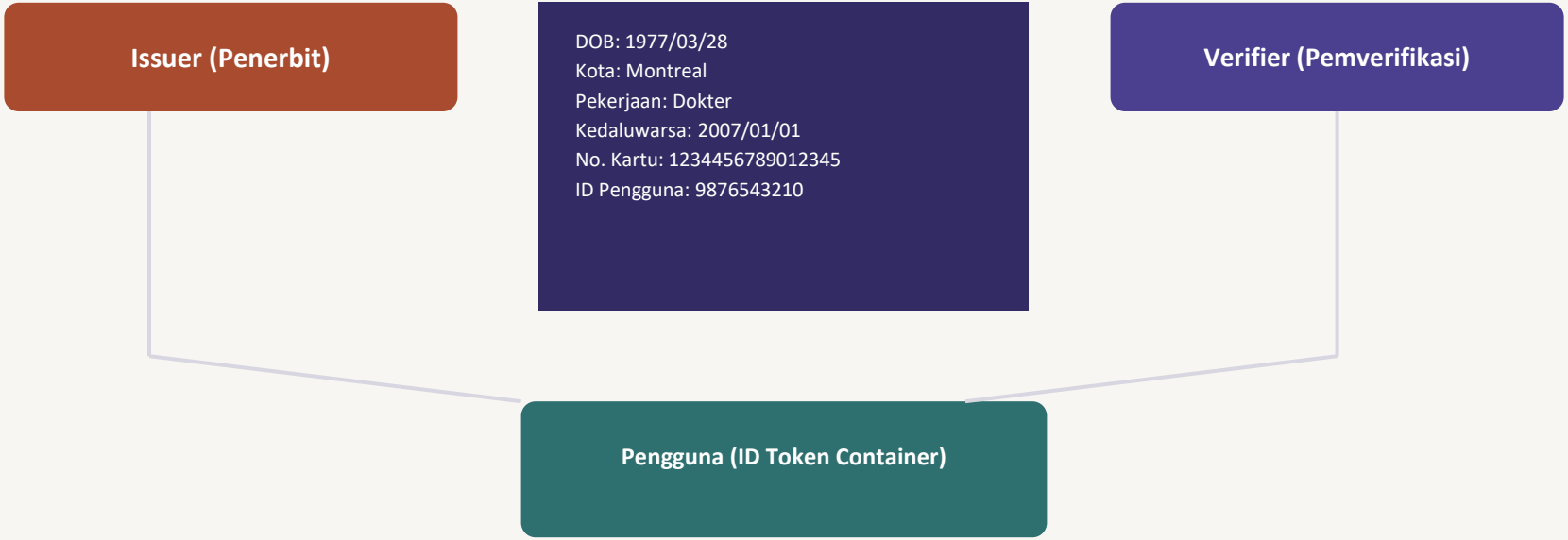
TEKNOLOGI

U-Prove SDK

"Multi-Party Security for User-Centric Identity"

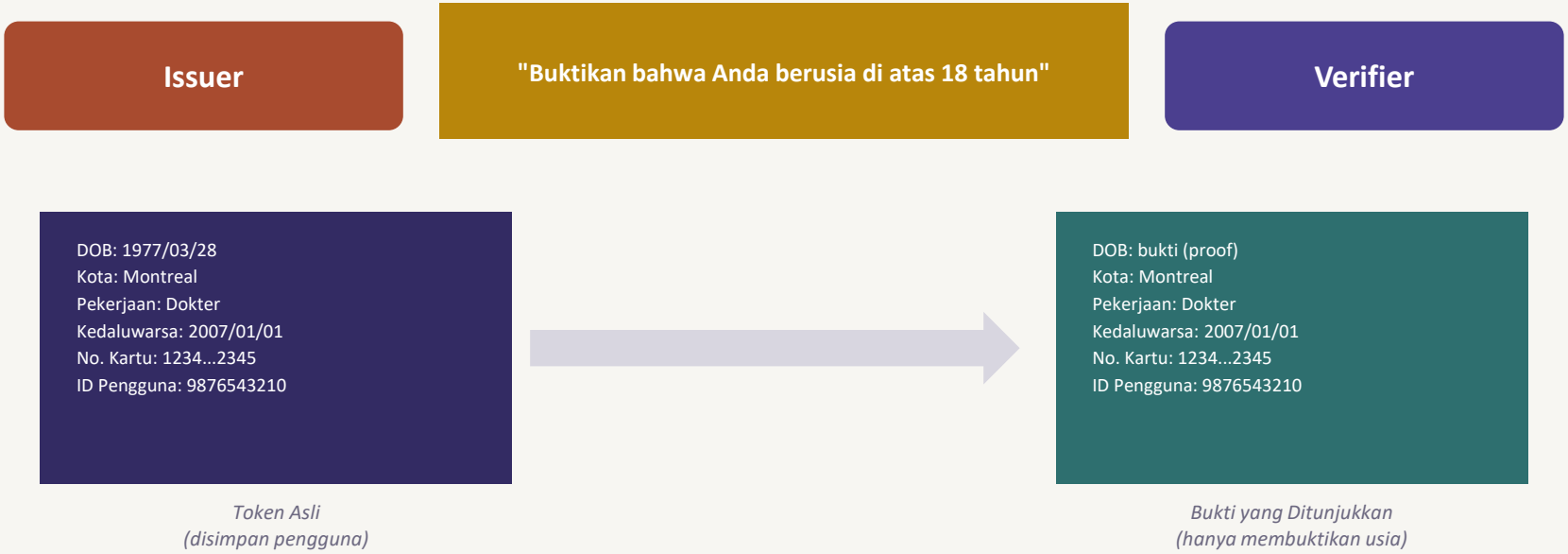
- U-Prove SDK dari Credentica membawa keamanan multi-pihak (multi-party security) dan skalabilitas sistem superior untuk identitas dan akses berpusat pada pengguna.
- Menggunakan teknologi ID Token berbasis kriptografi mutakhir (state-of-the-art) yang telah diverifikasi oleh pakar keamanan kriptografi terkemuka di dunia.
- Memungkinkan manajemen identitas kritis (privacy-critical identity management) tanpa memerlukan keterlibatan langsung dari penyedia identitas pusat pada setiap transaksi.
- Fitur utama: protected assertions, privacy, minimal disclosure, off-line transactions, accountability, data signing, dan hardware-bound assertions.

ID Token: Para Pelaku (Issuer, Verifier, User)



Sebuah ID Token berisi atribut identitas pengguna dan disimpan dalam wadah (container) milik pengguna, diterbitkan oleh Issuer dan ditunjukkan kepada Verifier saat diperlukan.

Pengungkapan Selektif: "Buktikan Usia di Atas 18 Tahun"



Pengguna hanya mengungkapkan atribut "DOB" sebagai bukti (proof) usia — tanpa membocorkan tanggal lahir aslinya kepada Verifier.

Membuktikan Beberapa Atribut Sekaligus

- Pengguna dapat membuktikan bahwa usianya di atas 18 tahun DAN bahwa ID Token belum kedaluwarsa — tanpa mengungkap tanggal lahir atau tanggal kedaluwarsa yang sebenarnya.
- Pengguna juga dapat membuktikan bahwa dirinya seorang dokter, apoteker, atau penyedia asuransi kesehatan — tanpa mengungkap identitas lengkap lainnya, seperti nomor kartu atau ID pengguna.
- Prinsip ini disebut minimal disclosure: hanya atribut yang relevan dengan permintaan Verifier yang diungkapkan, sisanya tetap tersembunyi dalam bentuk bukti kriptografis (cryptographic proof).

Jejak Audit yang Tidak Dapat Dipalsukan

- Verifier mencatat interaksi (misalnya, "seorang dokter dari Montreal mengunjungi saya") tanpa dapat mengidentifikasi pengguna secara spesifik.
- Auditor dapat memeriksa jejak transaksi ini di kemudian hari untuk memverifikasi keabsahan klaim (misalnya, "seorang dokter mengunjungi saya") tanpa membongkar identitas penuh pengguna, kecuali diperlukan secara sah.
- Pendekatan ini menyeimbangkan antara akuntabilitas (accountability) dan privasi — audit tetap dapat dilakukan tanpa mengorbankan kerahasiaan identitas pengguna dalam operasi normal.

Pencabutan Berbasis Identitas (Revocation)

"Buktikan bahwa ID Pengguna Anda tidak ada dalam daftar hitam (blacklist) saya"

- Verifier dapat memelihara daftar hitam (blacklist) berisi ID pengguna yang telah dicabut haknya atau disalahgunakan.
- Pengguna membuktikan (melalui bukti kriptografis) bahwa ID-nya TIDAK termasuk dalam daftar hitam tersebut, tanpa perlu mengungkap ID pengguna yang sebenarnya kepada Verifier.
- Mekanisme ini memungkinkan pencabutan akses secara efektif sambil tetap menjaga privasi pengguna yang identitasnya sah dan tidak masuk daftar hitam.

ID Token Berbasis Perangkat & Tanda Tangan Digital

ID Token Berbasis Perangkat

- ID Token dapat disimpan dan dikelola langsung pada perangkat keras pengguna (mis. kartu pintar/smart card atau perangkat mobile), bukan hanya perangkat lunak.
- Kunci privat terikat pada perangkat (hardware-bound), sehingga lebih tahan terhadap pencurian atau duplikasi kredensial.

Menandatangani Data Apa Pun

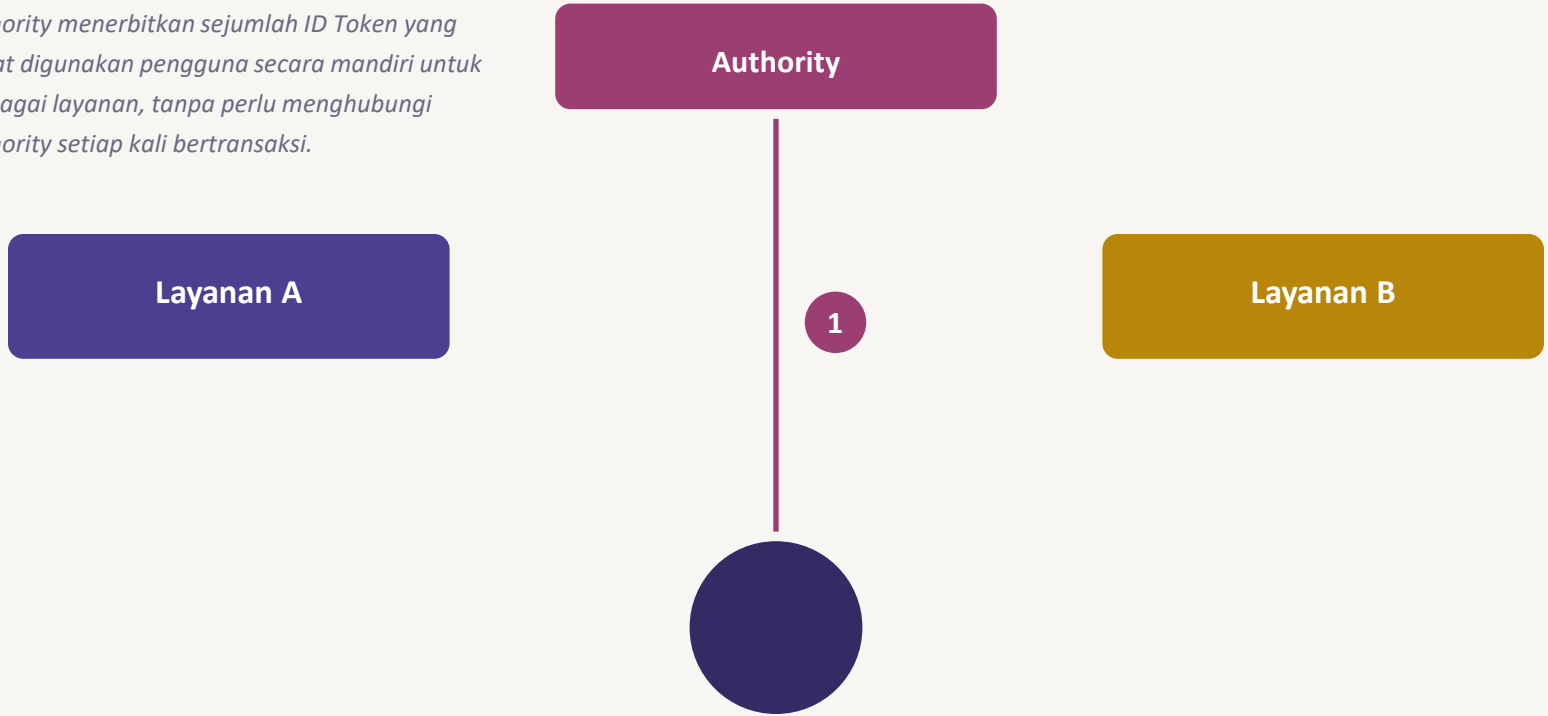
- Selain membuktikan atribut identitas, ID Token juga dapat digunakan untuk menandatangani dokumen atau data apa pun secara digital (mis. "Silakan tanda tangani dokumen ini").
- Tanda tangan yang dihasilkan tetap dapat diverifikasi keasliannya sekaligus menjaga privasi penandatangan sesuai kebutuhan.

BAGIAN 3

Identitas Berpusat Pengguna dengan ID Token

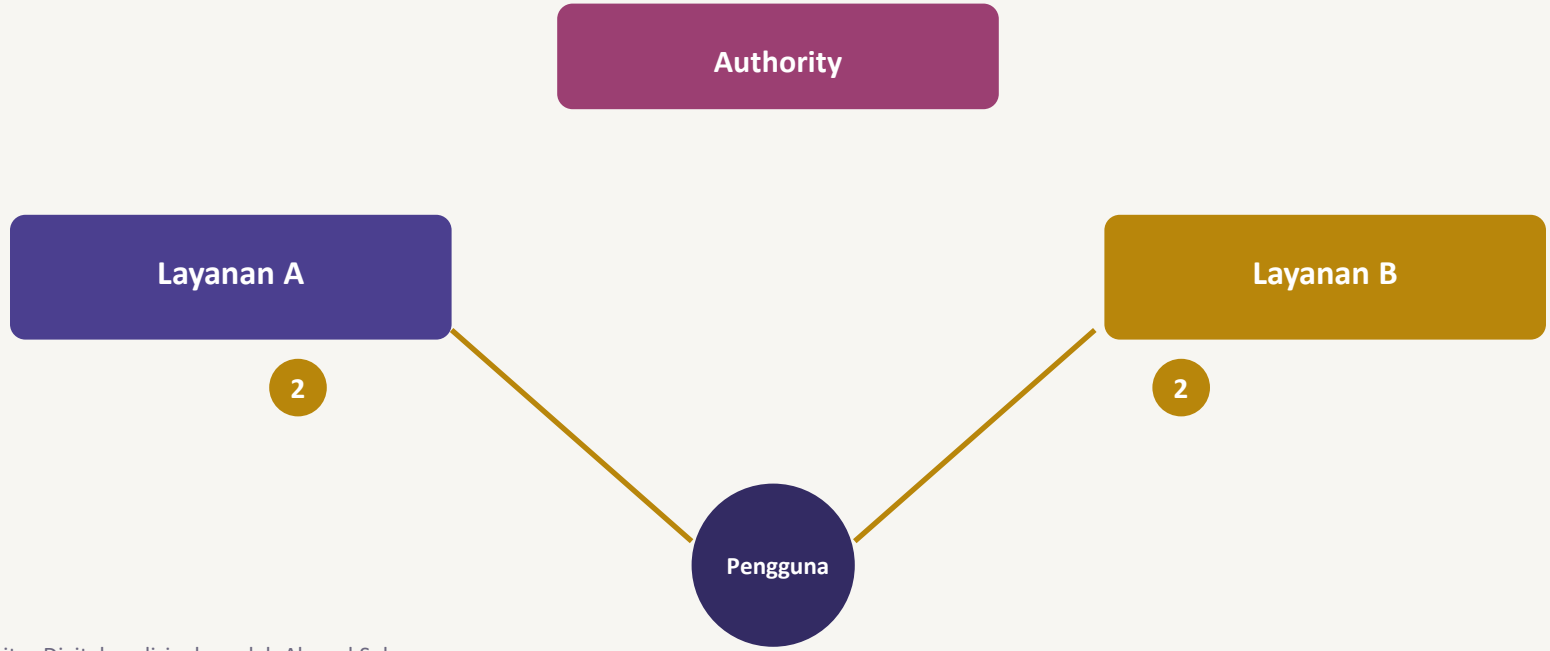
Langkah 1: Penerbitan Token oleh Authority

Authority menerbitkan sejumlah ID Token yang dapat digunakan pengguna secara mandiri untuk berbagai layanan, tanpa perlu menghubungi Authority setiap kali bertransaksi.



Langkah 2: Pengguna Menunjukkan Token ke Layanan

Pengguna menunjukkan token (atau bukti turunannya) langsung ke Layanan A dan Layanan B. Masing-masing layanan memverifikasi keabsahan token tanpa perlu menghubungi Authority.



MANFAAT PRIVASI

Token Tidak Dapat Ditautkan (Unlinkable)

- Setiap kali pengguna menunjukkan token ke layanan berbeda, token tersebut menghasilkan bukti unik yang berbeda — sehingga Layanan A dan Layanan B TIDAK dapat membandingkan catatan mereka untuk menyimpulkan bahwa mereka melayani pengguna yang sama.
- Bahkan jika Layanan A dan Layanan B serta Authority berkolusi (bekerja sama secara curang), mereka tetap tidak dapat menautkan (link) transaksi-transaksi pengguna yang sama menjadi satu profil gabungan.
- Ini adalah keunggulan privasi utama dibanding identitas terfederasi konvensional, di mana IdP pusat berpotensi melacak seluruh aktivitas pengguna di berbagai layanan.

RISIKO TANPA PERLINDUNGAN INI

Jika Token Dapat Ditautkan: Risiko Profil Gabungan

Tanpa mekanisme unlinkability, pihak-pihak yang berkolusi dapat menautkan berbagai pengenal (identifier) milik pengguna yang sama menjadi satu profil gabungan yang mengungkap lebih banyak informasi daripada yang dimaksudkan pengguna.

Layanan A: Tabel ID ↔ Layanan

ID: a349b71 → Layanan A
ID: 82cd711 → Layanan B
ID: 5a91fe02 → (tidak tertaut)

Layanan B: Tabel No. SIM ↔ ID

SIM: ABCDE... → 7f4d2201
SIM: FGHIJ... → 82cd711
SIM: KLMNO... → 5d1921b

Dengan menautkan ID "82cd711" yang muncul di kedua tabel, pihak yang berkolusi dapat mengetahui bahwa pengguna yang sama menggunakan Layanan A dan Layanan B — sesuatu yang seharusnya tetap privat.

KESIMPULAN

Takeaways

- Model identitas berkembang dari silo yang terisolasi, menuju federasi, hingga model yang berpusat pada pengguna — masing-masing memiliki trade-off antara kemudahan dan privasi.
- Teknologi ID Token berbasis kriptografi (seperti U-Prove) memungkinkan pengungkapan atribut secara selektif, jejak audit yang aman, dan pencabutan akses — tanpa mengorbankan privasi pengguna.
- Sifat unlinkability antar-layanan menjadi kunci untuk mencegah profil gabungan yang tidak diinginkan, bahkan ketika pihak-pihak yang terlibat berpotensi berkolusi.