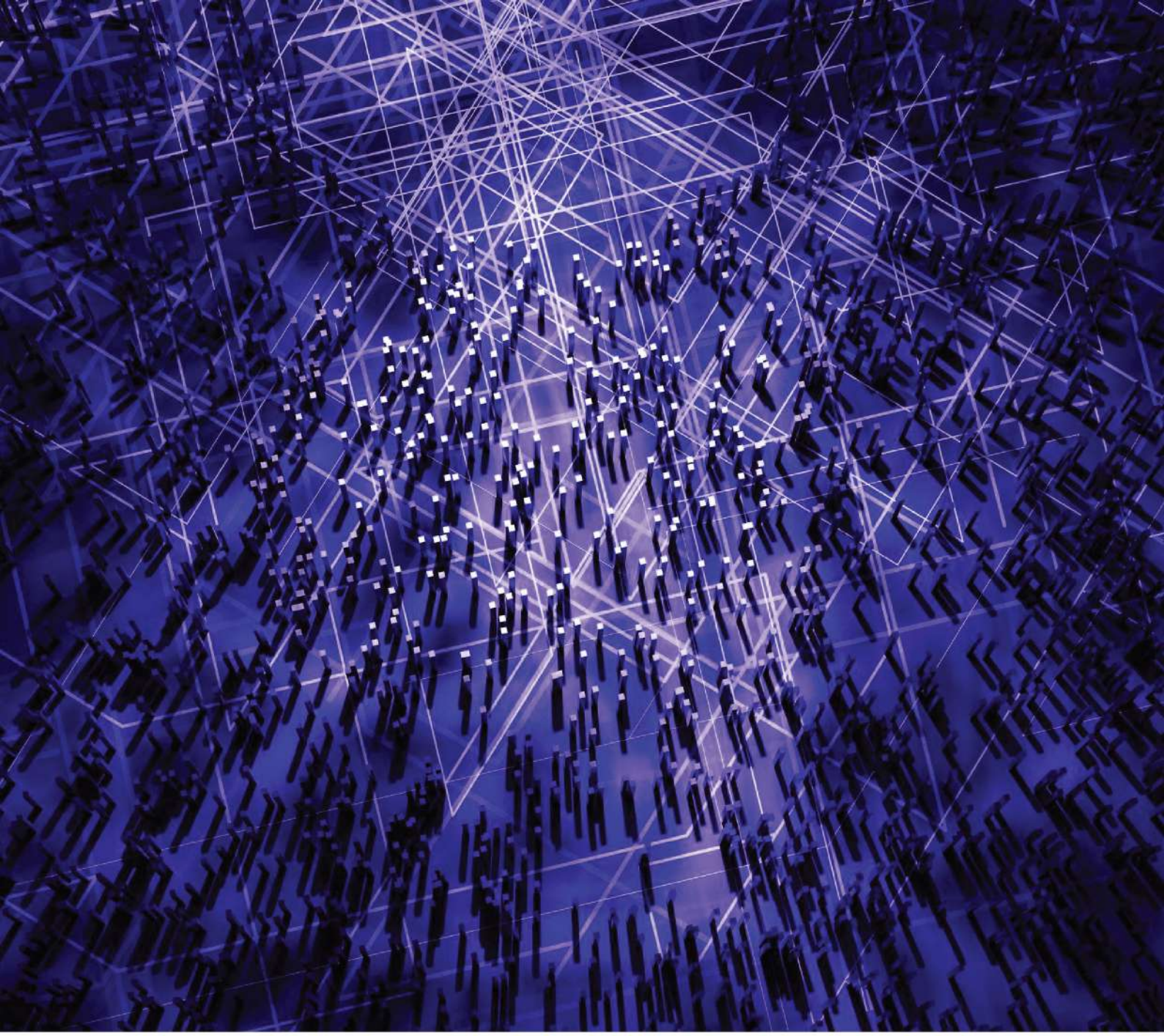


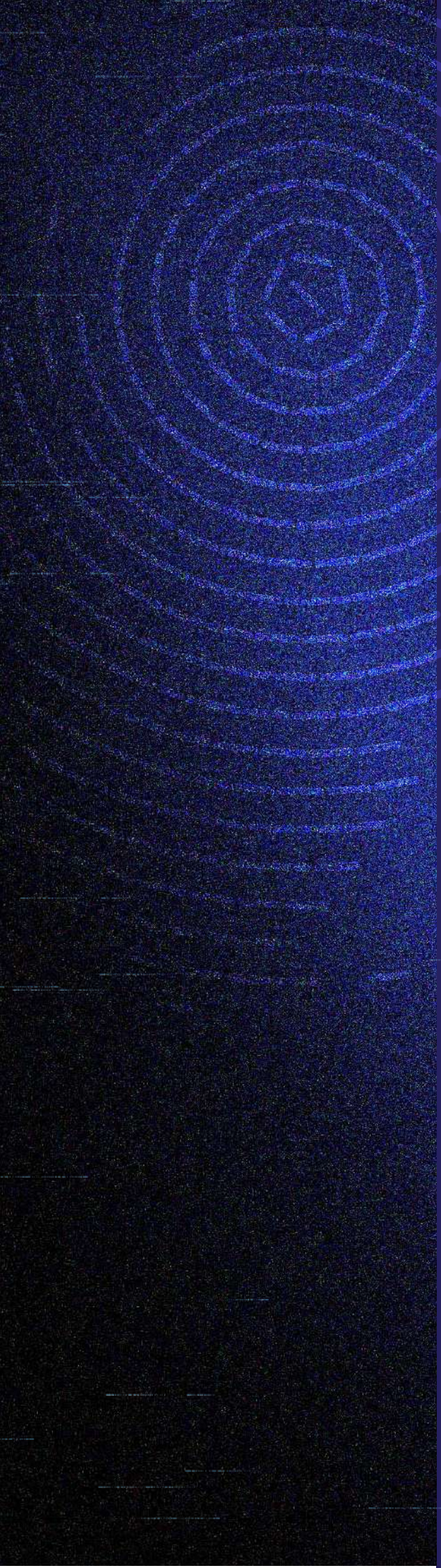
Proof of Human

Membangun Jaringan Manusia untuk Kepercayaan Digital dan Ketahanan terhadap Penipuan di Asia Pasifik

Desember 2025

Japan Trust & Safety Association
一般社団法人トラスト＆セーフティ協会

Southeast Asia
Public Policy Institute



Tentang White Paper ini

White paper ini disusun melalui penelitian oleh Southeast Asia Public Policy Institute bekerja sama dengan Japan Trust & Safety Association (JTSA) dengan dukungan dari Tools for Humanity. Fokus utama laporan ini adalah untuk mengetahui tingkat kepercayaan digital (digital trust) di kawasan Asia Pasifik. Informasi dan analisis yang disajikan berdasarkan wawancara dengan pemangku kepentingan yang relevan, informasi publik, dan analisis oleh para penulis. Kontribusi strategis JTSA—khususnya pandangan dari Kiyotaka Tanaka mengenai tata kelola, interoperabilitas, dan implementasi Proof of Human (PoH) berbasis risiko—sangat membantu penyusunan makalah ini.

White paper ini tidak mewakili pandangan Tools for Humanity. Laporan ini juga tidak dimaksudkan untuk menjadi tinjauan menyeluruh tentang kebijakan, undang-undang, atau peraturan dan seharusnya digunakan dengan hati-hati dan mempertimbangkan ruang lingkup serta keterbatasannya.

Daftar Isi

Ringkasan Eksekutif

Penipuan daring (online scams) telah berkembang menjadi jaringan industri kejahatan lintas negara. Nilai ekonomi kejahatan siber global kini melebihi 10 triliun dolar AS, dengan kerugian akibat penipuan mencapai lebih dari 1 triliun dolar AS setiap tahunnya. Selain kerugian finansial, penipuan mengikis kesehatan mental, kepercayaan publik, dan menguras sumber daya penegak hukum. Kawasan Asia-Pasifik sering menjadi target utama dan pusat operasional: Asia Tenggara menjadi pusat operasi penipuan berskala besar, yang sering kali terkait dengan perdagangan manusia, sementara negara maju seperti Jepang dan Korea menjadi target penipuan investasi dan pencurian identitas. Masalah ini telah menjadi masalah tingkat regional, sehingga membutuhkan respons yang terkoordinasi dari berbagai negara.

Kecerdasan artifisial (AI) digunakan untuk menirukan suara dan video (deepfake) untuk mempersuasi korban penipuan; AI juga digunakan untuk membuat akun secara otomatis yang memungkinkan penipu menjangkau masyarakat secara luas; kripto serta pembayaran instan mempercepat monetisasi kejahatan. Namun, teknologi yang sama juga bisa menjadi solusi jika digunakan untuk memperkuat sistem keamanan seperti verifikasi identitas yang lebih baik, sinyal keaslian, dan perlindungan data yang menjaga privasi, yang didukung oleh tata kelola dan transparansi untuk mencegah risiko baru.

Upaya penegakan hukum dan peningkatan kesadaran perlu dilakukan, tetapi itu saja tidak cukup ketika para penjahat dapat dengan mudah menciptakan ribuan identitas palsu secara otomatis. Perkembangan yang berkelanjutan membutuhkan dua lapisan kepercayaan digital yang mampu menutup celah yang sering dimanfaatkan oleh penipu:

- Identitas Digital (ID Digital): Digunakan untuk menjawab pertanyaan "Siapakah Anda?" Ini adalah kredensial non-anonim yang mampu melakukan prosedur KYC (Know Your Customer) untuk bidang yang diregulasi (keuangan, e-gov).
- Proof of Human (PoH): Digunakan untuk menjawab pertanyaan "Apakah Anda manusia sungguhan?" Sistem ini digunakan untuk menjaga privasi dan dapat digunakan di berbagai platform di mana pengungkapan identitas secara penuh tidak diperlukan atau diinginkan.

PoH bukanlah pengganti Identitas Digital. PoH adalah lapisan pelengkap yang memperluas keamanan di ruang digital yang sering menjadi sasaran penipuan (media sosial, aplikasi pengiriman pesan, lokapasar/marketplace). PoH juga mengurangi kemungkinan dibuatnya akun palsu dan mencegah penyalahgunaan yang digerakkan oleh bot, sembari tetap menjaga privasi pengguna. Perkembangan terkini menunjukkan perlunya menerapkan PoH dalam kerangka kerja berbasis kepercayaan dan keamanan. Hal ini untuk memastikan bahwa sistem keamanan yang ada dapat mengatasi otomatisasi dan penyalahgunaan dalam skala besar. Namun, PoH tidak dapat diartikan sebagai alat untuk mengetahui niat atau tingkat kejujuran pengguna.

Pemerintah di Asia Pasifik telah membangun fondasi identitas digital yang memperkuat prinsip KYC dan akuntabilitas di sektor yang diregulasi. Tetapi, sebagian besar aktivitas penipuan justru berasal dari ruang yang tidak diregulasi di mana Identitas Digital tidak berlaku, seperti media sosial, aplikasi pengiriman pesan, dan lokapasar. Di sinilah PoH berperan: melalui mekanisme seperti token manusia yang menjaga privasi dan verifikasi berbasis perangkat, PoH dapat membatasi pembuatan akun palsu secara massal, mengganggu operasi penipuan yang digerakkan oleh bot, dan memperkuat jaringan manusia otentik sebelum korban menjadi sasaran. Keberhasilan berbagai teknologi ini memerlukan pengamanan yang jelas, kontrol pengguna, dan struktur tata kelola yang dapat mencegah penyalahgunaan, melindungi anonimitas, dan menjaga kepercayaan publik.

Contoh Kasus

Jepang — My Number: Nomor identitas unik dalam skala besar yang diverifikasi oleh negara. Tetapi penggunaannya menghadapi tantangan insiden penanganan data. Contoh ini merupakan kandidat utama untuk model campuran (hybrid) yang menggabungkan identitas (ID) pemerintah dengan PoH untuk verifikasi yang tetap menjaga privasi serta dapat digunakan selain untuk layanan pemerintah.

Korea Selatan — Rezim nama-asli (Real-name regime): Integrasi mendalam di sektor keuangan, telekomunikasi, dan e-gov secara efektif berlaku sebagai proksi PoH. Cara ini dikhawatirkan mengganggu privasi/kebebasan sipil, sehingga mendorong minat untuk mengadopsi otentikasi terdesentralisasi yang dikendalikan oleh pengguna.

Malaysia — MyDigital ID (dalam tahap peluncuran): Kredensial yang terhubung dengan biometrik dan data registri nasional. Cara ini dirancang sangat selaras dengan prinsip-prinsip PoH, tetapi membutuhkan perlindungan yang kuat dan kepercayaan publik yang tinggi agar dapat berkembang.

Filipina — PhilSys (skala cepat): Mengunduh identitas digital dan verifikasi elektronik. Cara ini telah diadopsi secara massal dengan cepat dan mampu menunjukkan fungsionalitas operasional seperti PoH. Penggunaannya bersamaan dengan kebutuhan untuk menjaga tata kelola dan pendidikan pengguna berjalan dengan cepat.

Ketahanan terhadap penipuan yang efektif membutuhkan jaminan berlapis: verifikasi identitas untuk interaksi dalam sektor-sektor yang diregulasi dan platform terbuka yang diperkuat oleh mekanisme pembuktian manusia dengan metode yang tetap menjaga privasi. Transparansi, interoperabilitas, dan kontrol pengguna adalah pendorong utama. Mekanisme tata kelola netral—baik pada badan standar, perantara industri, atau kerangka kerja multipihak—akan sangat penting untuk mengimplementasikan persyaratan nasional ke dalam praktik operasional untuk platform global.

Rekomendasi Kebijakan

Mengintegrasikan Identitas Digital dan PoH ke dalam strategi pencegahan penipuan: Memasukkan PoH dalam bidang keuangan, perdagangan elektronik (e-commerce), dan komunikasi untuk mencegah pencurian identitas, identitas palsu, dan penyalahgunaan bot. Penerapannya harus berbasis kepercayaan dan keamanan serta perlindungan yang mencegah ketergantungan berlebihan.

Mendukung standar yang menjaga privasi dan interoperabilitas: Memadukan jaminan biometrik/kredensial dengan teknik kriptografi (misalnya, zero-knowledge proofs) untuk melindungi anonimitas dan memungkinkan penggunaan lintas batas, sambil tetap memastikan PoH tidak dapat digunakan untuk pelacakan atau pemprofilan.

Dialog dan koordinasi kebijakan regional: Menggunakan platform seperti Dewan Penasihat Bisnis APEC (APEC Business Advisory Council), Prinsip Tingkat Tinggi G20 untuk Inklusi Keuangan Digital (G20 High-Level Principles for Digital Financial Inclusion), dan berbagai inisiatif ekonomi digital PBB untuk menyelaraskan tujuan, berbagi studi kasus, dan menguji metode verifikasi yang diaktifkan PoH di berbagai sektor, termasuk uji coba (sandbox testing) untuk menilai kegunaan, tingkat inklusi, dan proporsionalitas.

Penipuan mengungkap adanya penurunan kepercayaan struktural. Gabungan arsitektur Identitas Digital dan Proof of Human —yang diimplementasikan dengan privasi, tata kelola, dan interoperabilitas yang kuat—dapat membuat biaya untuk penyalahgunaan dalam skala besar menjadi lebih mahal sekaligus melindungi hak pengguna, mempercepat Asia menuju ekonomi digital yang lebih aman dan inklusif.

Pendahuluan: Epidemik Penipuan dan Celah Kebijakan (Policy Gap)

Sejalan dengan adopsi teknologi digital oleh masyarakat, kejahatan daring juga semakin canggih dan meningkat pesat. Nilai ekonomi kejahatan siber global kini mencapai lebih dari 10 triliun dolar AS, Ini setara dengan ekonomi terbesar ketiga di dunia berdasarkan PDB.[1] Penipuan adalah jenis kejahatan siber yang spesifik dan terus berkembang. Setiap tahunnya, konsumen kehilangan lebih dari 1 triliun dolar AS akibat penipuan.[2] Namun, dampak negatifnya lebih dari sekadar kerugian ekonomi: korban mengalami gangguan mental dan penurunan kesejahteraan, menurunnya kepercayaan terhadap layanan dan ekonomi digital, dan sumber daya publik banyak dialihkan untuk penegakan hukum, membangun kesadaran, dan upaya keamanan siber nasional.[3]

Peran Ganda Asia

Dalam pusaran epidemi penipuan global ini, Asia Pasifik menonjol sebagai kawasan yang paling terdampak. Penipuan yang disebut ‘pig butchering’ (skema penipuan jangka panjang di mana pada awalnya penipu membangun kepercayaan terhadap korban), penipuan investasi atau asmara, di mana penipu menggunakan teknik rekayasa sosial untuk membina hubungan dengan korban dan menipu mereka agar melakukan pembayaran atau investasi, sangat marak terjadi. Penipuan ini sering kali dimulai melalui media sosial atau layanan pengiriman pesan yang dilakukan oleh sindikat kejahatan transnasional dalam skala besar dan biasanya dilakukan dari pusat penipuan khusus.

Asia Tenggara berada di pusat perekonomian gelap ini: wilayah yang belum diregulasi menjadi pusat operasi; ada pihak-pihak yang menjadi korban penipuan; ada juga yang terjebak sebagai pekerja, hingga tidak jarang melibatkan perdagangan manusia.[4,5]

Sementara itu, negara-negara maju di kawasan Asia Pasifik seperti Taiwan, Jepang, dan Korea Selatan juga terkait erat dengan dinamika ini: perekonomian mereka sangat terpercaya dan matang secara digital, sehingga konsumen dari negara-negara ini sering menjadi target penipuan investasi dan penipuan identitas. Mereka juga telah menyaksikan warga negara mereka sendiri dibujuk ke berbagai pusat penipuan di luar negeri.[6] Berbagai dinamika ini menunjukkan bagaimana krisis ini bukan hanya bersifat lokal, tetapi juga merupakan bagian dari tantangan yang saling terkait di seluruh Asia, sehingga membutuhkan respons terkoordinasi yang menghubungkan negara-negara maju dan negara-negara yang terkena dampak perdagangan manusia. [7]

Teknologi: sebagai pendorong sekaligus solusi

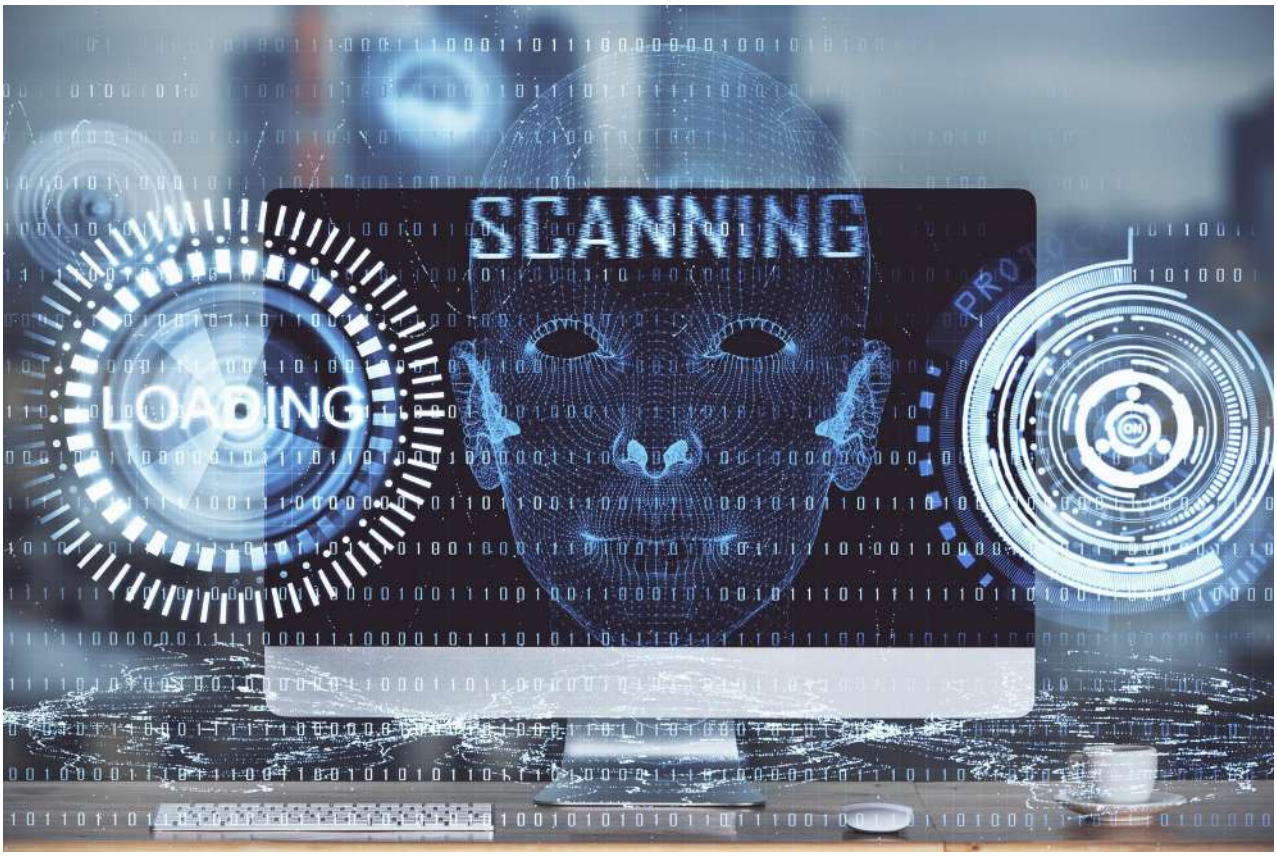
Teknologi telah mengubah ekonomi penipuan (economics of scamming) secara fundamental, dan bahkan pemerintah dengan sumber daya terbaik pun kesulitan untuk mengimbangi evolusi metode penipuan yang cepat.

Pertama, persuasi telah diindustrialisasi. Kecerdasan buatan, kloning suara, dan deepfake dipersenjatai untuk memfasilitasi penipuan. Data menunjukkan lebih dari 42 persen upaya penipuan sektor keuangan dikaitkan dengan AI.[8] Alat-alat ini dapat memberikan skrip, gambar, dan panggilan telepon yang sangat realistis dalam berbagai bahasa, memungkinkan skema "investasi" atau asmara jangka panjang dijalankan oleh operator yang relatif tidak terampil dan bekerja dengan mengikuti panduan yang disempurnakan melalui uji perbandingan (A/B testing).

Kedua, peningkatan kapasitas digital telah menjadi tidak terbatas: pembuatan akun otomatis, SIM farm (kumpulan kartu SIM yang terhubung ke satu server untuk mengirimkan banyak pesan), dan alat lintas platform memungkinkan tim kecil untuk menghubungi jutaan orang di media sosial, aplikasi pengiriman pesan, dan telepon dalam hitungan jam, sementara bot dan sistem rekomendasi dapat dimanipulasi untuk mengidentifikasi calon korban yang responsif.[9]

Ketiga, inovasi monetisasi penipuan telah meningkat pesat seperti melalui infrastruktur kripto, teknologi finansial (fintech), money-mule network (jaringan penipu yang membujuk orang menerima transfer hasil penipuan), dan gabungan lintas bidang yang memungkinkan pergerakan dan pengaburan dana (obfuscation of funds) dengan cepat, sementara pembayaran instan dan rezim KYC/KYB yang terfragmentasi membuat pencegahan penipuan di perbankan tradisional menjadi kurang cepat.[10]

Dampaknya adalah penurunan kepercayaan struktural dalam ekonomi digital: para penjahat mengadopsi dan menyesuaikan alat-alat baru lebih cepat daripada kemampuan pemerintah dan regulator untuk meresponsnya.



Namun, teknologi yang memungkinkan penyalahgunaan, jika diterapkan dalam skala besar dengan pengamanan, justru dapat memulihkan kepercayaan.

Penguatan jaminan identitas dan entitas digital—melalui verifikasi individu yang tetap menjaga privasi, pemeriksaan keamanan perangkat, serta validasi identitas bisnis; pemantauan reputasi nomor ponsel (SIM); serta penerapan standar keamanan yang lebih ketat untuk transaksi berisiko tinggi—dapat mempersulit dan meningkatkan biaya bagi pelaku kriminal dalam mencari korban secara massal.

Penerapan sinyal keaslian (otentisitas) pada konten dan komunikasi—seperti penggunaan jejak kriptografi untuk melacak asal gambar dan video, penerapan sistem verifikasi identitas penelepon atau pengirim pesan, serta pengawasan ketat terhadap integritas iklan dan akun dapat secara efektif menekan keberhasilan aksi pencurian identitas.

Pertukaran data atau sinyal keamanan yang menjaga privasi di berbagai platform dan jaringan pembayaran dapat membantu mendeteksi kejahatan yang terorganisir. Selain itu, evaluasi risiko transaksi secara langsung (real-time) serta penerapan masa tunggu atau hambatan “cool off” (seperti konfirmasi ulang penerima dana, pemeriksaan mendalam, dan penundaan pencairan dana/settlement untuk transfer yang mencurigakan) mampu meminimalkan kerugian saat transaksi dilakukan.

Penerapan model perlindungan yang berfokus pada korban—termasuk mekanisme penghapusan konten ilegal yang cepat, proses pemulihan dana yang lebih singkat, serta prosedur jelas untuk mengidentifikasi pekerja paksa sebagai korban kejahatan—harus menjadi pelengkap penegakan hukum guna memutus rantai eksploitasi.[11]

Dengan demikian, teknologi berperan ganda sebagai pendorong aktivitas kriminal sekaligus menjadi bagian penting dari solusinya. Pemerintah, penyedia platform, dan lembaga keuangan harus terus mengadopsi serta memperbarui sistem pertahanan digital agar dapat mengimbangi kecepatan inovasi para pelaku kriminal. Hal ini penting karena maraknya penipuan bukan sekadar masalah kejahatan siber biasa, melainkan pertanda adanya krisis kepercayaan struktural yang mendalam dalam ekonomi digital.[12]

Jika penipuan mengungkapkan kerapuhan kepercayaan daring, maka identitas digital (ID) yang andal adalah salah satu alat paling jelas yang tersedia untuk memperbaikinya. Dengan memberikan jaminan yang dapat diverifikasi tentang siapa yang berada di balik transaksi atau interaksi, identitas digital meningkatkan biaya penyalahgunaan sekaligus mendukung ekonomi digital yang lebih aman. Bagian selanjutnya akan membahas pemecahan masalah yang dirancang oleh identitas digital, teknologi yang terlibat, dan respons kebijakan yang muncul di wilayah tersebut.

Dua Lapisan Kepercayaan Digital: Identitas Digital dan Proof of Human

Mengatasi penipuan membutuhkan sistem kepercayaan berlapis. Penegakan hukum dan kesadaran masyarakat sangat penting, tetapi kemajuan yang berkelanjutan bergantung pada mekanisme verifikasi identitas dan otentisitas yang mampu menutup celah yang sering dieksploitasi penjahat. Identitas Digital (ID Digital) dan Proof of Human (PoH) mewakili dua lapisan infrastruktur kepercayaan yang pada dasarnya berbeda tetapi saling melengkapi. Identitas Digital mampu menjawab pertanyaan "Siapa Anda?" dengan cara menghubungkan individu dengan identitas di dunia nyata yang terverifikasi dan diakui oleh bank dan pemerintah, sementara Proof of Human menjawab pertanyaan "Apakah Anda manusia?" dengan mengonfirmasi manusia tanpa mengungkapkan identitas. Yang satu bersifat tidak anonim dan cocok untuk diterapkan dalam ranah yang diregulasi, seperti perbankan dan e-government; yang lain bersifat anonim, tetapi dapat diverifikasi, sehingga dapat mengamankan ruang digital terbuka di mana pengungkapan identitas secara lengkap tidak diperlukan atau diinginkan. Keduanya bersama-sama menciptakan fondasi yang seimbang yang mendukung akuntabilitas dan privasi dalam ekonomi digital.

Proof of Human bukanlah pengganti sistem identitas digital nasional; tetapi sebagai lapisan pelengkap yang menjaga privasi dan memperluas kepercayaan ke berbagai bagian ruang digital di mana verifikasi identitas secara penuh tidak memungkinkan atau tidak diinginkan.

Berbagai bentuk teknologi identitas digital

Solusi identitas digital hadir dalam berbagai bentuk, masing-masing mengatasi risiko yang berbeda:

Sistem identitas digital berbasis kredensial. Sistem ini menggunakan bukti identitas resmi yang diterbitkan secara digital oleh lembaga terpercaya, seperti pemerintah, bank, penyedia layanan seluler, atau universitas untuk dapat memverifikasi identitas seperti nama, usia, atau kewarganegaraan. Data ini disimpan dengan aman dalam dompet digital dan dapat digunakan untuk berbagai layanan tanpa perlu memindai dokumen fisik berulang kali. Metode ini jauh lebih praktis dan lebih baik dalam menjaga privasi dibandingkan sekadar menggunakan kredensial login tradisional.[13]

Otentikasi biometrik. Teknologi ini memastikan bahwa orang yang mengakses layanan benar-benar individu yang terdaftar dengan memverifikasi ciri fisik atau perilaku unik, seperti sidik jari atau pemindaian wajah. Biometrik sangat efektif untuk mencegah akses ilegal, bahkan jika perangkat atau kata sandi pengguna telah dicuri. Namun, perlu dipahami bahwa biometrik berfungsi untuk mengonfirmasi bahwa pengguna adalah orang yang sama dengan yang terdaftar, namun tidak untuk menetapkan identitas seseorang secara hukum.[14]

Model identitas digital campuran (hybrid). Model ini menggabungkan berbagai faktor keamanan, seperti kredensial resmi pemerintah yang dipadukan dengan otentikasi biometrik. Gabungan ini menciptakan identitas digital dengan tingkat jaminan keamanan yang sangat tinggi yang dapat digunakan secara fleksibel di berbagai platform. Sistem ini dirancang untuk mendukung transparansi, keamanan yang kuat, dan kontrol privasi yang lebih baik.[15]

Semua dirancang untuk memenuhi prinsip KYC yang tidak anonim. Tujuannya adalah untuk memastikan adanya ketertelusuran, kepatuhan, dan akuntabilitas dalam ekosistem yang teregulasi.

Respons Kebijakan di Asia Pasifik

Teknologi identitas digital tidak dapat berhasil tanpa dukungan; teknologi ini membutuhkan kerangka kebijakan pendukung yang menetapkan standar, menjamin privasi, dan mendorong adopsi yang luas. Dalam praktiknya, hal ini berarti:

- Kejelasan regulasi sehingga identitas digital memiliki bobot hukum dalam transaksi keuangan, kontrak, dan layanan publik.
- Pengamanan yang kuat untuk melindungi data pribadi, dengan persyaratan penyimpanan yang aman, penggunaan terbatas, dan mekanisme perbaikan/ganti rugi jika terjadi penyalahgunaan.
- Adopsi sektor publik-swasta dan lintas sektor, memastikan bahwa identitas diakui tidak hanya oleh pemerintah tetapi juga oleh platform, bank, dan layanan dasar (utilitas) yang sering menjadi target penipuan.

Di seluruh Asia Tenggara, pemerintah terus memajukan sistem identitas digital sebagai fondasi untuk membangun ekonomi digital yang lebih terpercaya.

Platform Identitas Digital Nasional (NDID) Thailand menghubungkan bank, operator telekomunikasi, dan lembaga negara dalam kerangka kerja terfederasi.[16]

Indonesia dan Filipina meluncurkan program identitas nasional elektronik yang digunakan untuk inklusi keuangan dan layanan sosial.

Vietnam telah mulai menggunakan verifikasi biometrik ke dalam portal e-government-nya.

Meskipun tingkat kematangannya bervariasi, kebijakan regional bergeser dari membangun sistem nasional menjadi mengeksplorasi interoperabilitas. Para pembuat kebijakan semakin menyadari bahwa mobilitas, migrasi, dan arus perdagangan membutuhkan identitas yang dapat dikenali lintas batas, bukan hanya di dalam negeri.

Di negara-negara dengan ekonomi yang lebih maju, kerangka kerja identitas nasional yang komprehensif telah bergerak menuju integrasi yang lebih dalam.

SingPass Singapura menjadi landasan akses ke perbankan, layanan kesehatan, dan perdagangan elektronik (e-commerce). [17]

Korea Selatan tengah memperluas sistem registrasi penduduk nasionalnya menjadi sepenuhnya digital yang mengintegrasikan layanan e-government, transaksi keuangan, dan otentikasi seluler.

Sistem “My Number” Jepang memberikan nomor unik 12 digit kepada setiap penduduknya. Nomor tersebut semakin dikaitkan dengan layanan kesehatan, perpajakan, dan administrasi.[18] Jepang juga sedang mengupayakan perluasan kegunaannya ke layanan keuangan dan pengakuan lintas batas.

Berbagai contoh di atas berbeda dalam cakupan dan kecepatan implementasinya, tetapi sama-sama menggambarkan bagaimana pemberian kredensial skala nasional dapat berkembang melampaui login yang aman (nama pengguna dan kata sandi) untuk menjadi tulang punggung ekonomi digital, sekaligus menawarkan contoh-contoh kasus kepada pemerintah negara-negara ASEAN yang mempertimbangkan implementasi domestik atau interoperabilitas regional.

Pada saat yang sama, berbagai pengalaman ini menyoroti bahwa tindakan pemerintah saja tidak cukup. Efektivitas Identitas Digital pada akhirnya bergantung pada integrasinya di seluruh ekosistem digital yang lebih luas melalui kerja sama antara pemerintah, lembaga keuangan, dan platform teknologi.

Peran Identitas Digital dalam Memerangi Penipuan

Teknologi Identitas Digital termasuk alat sistemik yang paling menjanjikan untuk melawan penipuan dan kecurangan. Melalui otentikasi orang, perangkat, dan organisasi dengan cara terverifikasi dan non-anonim, sistem Identitas Digital dapat mengurangi pencurian identitas, membatasi anonimitas, dan meningkatkan biaya penyalahgunaan. Meskipun bukan solusi ajaib, sistem ini membentuk tulang punggung kepercayaan digital yang mampu melakukan KYC (Know Your Customer), dan memastikan bahwa transaksi dan layanan memang diakses oleh individu atau entitas sesungguhnya yang bertanggung jawab.

Menutup celah yang dimanfaatkan oleh para penipu

Penipuan berkembang pesat karena adanya celah dalam verifikasi. Para penipu menggunakan bot dan akun palsu untuk menyebarkan pesan dengan biaya yang sangat rendah, menggunakan deepfake dan klon suara untuk meniru individu yang dipercaya, dan membajak akun yang sah untuk menipu korban. Otentikasi yang lemah atau tidak konsisten di berbagai platform membuat berbagai serangan ini jauh lebih sering berhasil daripada seharusnya.

Identitas digital menutup celah ini dari sisi regulasi: dengan mengikat interaksi digital ke identitas yang terverifikasi, akan lebih sulit bagi para penjahat untuk beroperasi secara anonim dan lebih mudah bagi korban, bisnis, dan regulator untuk mempercayai dengan siapa mereka berurusan secara daring. Namun, sebagian besar penipuan berasal dari ruang yang tidak diregulasi, seperti media sosial, aplikasi pesan, dan lokapasar informal, di mana sistem KYC tidak berlaku. Menangani ruang-ruang ini membutuhkan pendekatan yang berbeda, seperti Proof of Human yang dapat menjaga privasi.

Namun, bahkan sistem Identitas Digital yang terkuat pun tidak dapat sepenuhnya mengatasi penipuan yang didorong oleh akun palsu dan penyalahgunaan otomatis. Celah ini telah mendorong minat yang semakin besar pada konsep-konsep baru, seperti Proof of Human, yang menelusuri cara-cara untuk memverifikasi bahwa pengguna itu nyata tanpa memerlukan identifikasi pribadi.

Proof of Human: Konsep dan Relevansi Kebijakan

Definisi 'Proof of Human'

Proof of Human (PoH) adalah pendekatan baru yang terus berkembang untuk memperkuat kepercayaan digital. PoH umumnya didefinisikan sebagai sebuah sistem yang dirancang untuk mencegah banyak identitas palsu, serta memberikan jaminan yang dapat diverifikasi bahwa pelaku daring adalah manusia sungguhan, bukan bot otomatis atau identitas palsu.[19] Tidak seperti pendaftaran akun sederhana atau CAPTCHA, PoH bertujuan untuk memberikan sinyal sifat manusia (humanness) yang dapat digunakan kembali, dapat dikenali di berbagai platform dan layanan tanpa mengungkapkan data pribadi secara berlebihan, hal ini menjadi dasar untuk jaringan manusia yang lebih tepercaya di seluruh ekosistem digital.

Yang terpenting, PoH tidak menggantikan atau bersaing dengan sistem identitas digital nasional. Sebaliknya, PoH melengkapi sistem tersebut dengan mengatasi masalah kepercayaan pada lapisan yang berbeda, yaitu memverifikasi bahwa pengguna adalah manusia, bukan menetapkan siapa pengguna tersebut.

Secara konsep, PoH berbeda dari lapisan jaminan digital lainnya. Kerangka kerja identitas digital tradisional menjawab pertanyaan "siapa Anda?" dengan menghubungkan individu dengan atribut yang diverifikasi seperti nama atau nomor registrasi nasional. Alat otentikasi seperti kata sandi atau kode multi-faktor melindungi akun setelah dibuat, tetapi tidak mencegah pembuatan profil palsu atau sintetis sedari awal. Selama hampir dua dekade, CAPTCHA mencoba mengisi celah tersebut dengan menguji apakah pengguna dapat memecahkan teka-teki sebagai bukti bahwa pengguna adalah manusia. Namun, efektivitasnya telah menurun karena bot dan alat AI semakin mengungguli manusia, menciptakan hambatan bagi pengguna yang sah. Sebaliknya, PoH menjawab pertanyaan sebelumnya "apakah Anda adalah manusia?", suatu bentuk jaminan yang selaras dengan upaya yang lebih luas dalam kredensial terverifikasi, mitigasi bot, dan apa yang disebut komunitas blockchain sebagai ketahanan terhadap serangan Sybil. Dalam hal ini, PoH merupakan bagian dari rangkaian inovasi yang lebih luas yang bertujuan untuk menyeimbangkan otentisitas, privasi, dan skalabilitas dalam ekosistem digital.

Bentuk Verifikasi PoH

Sistem Proof of Human (PoH) dapat diimplementasikan dengan beberapa cara, masing-masing menawarkan tingkat jaminan dan privasi yang berbeda. Tabel di bawah ini menguraikan bentuk-bentuk utama verifikasi PoH dan bagaimana cara kerjanya.

Jenis Verifikasi PoH	Cara Kerja	Pengalaman Pengguna	Contoh Kasus Penggunaan
Berbasis biometrik (privasi terjaga)	Pemeriksaan keaktifan satu kali (misalnya, berkedip/menoleh). Sistem mengeluarkan "token manusia" kriptografis tanpa menyimpan atau membagikan data biometrik.	Verifikasi singkat satu kali, mirip dengan membuka kunci ponsel; tidak ada data identitas yang diungkapkan.	Mencegah pembuatan akun palsu secara massal; PoH dengan jaminan tingkat tinggi untuk platform yang menangani transaksi keuangan atau berisiko tinggi.
Berbasis perangkat/ piranti keras	Verifikasi perangkat mengonfirmasi perangkat asli, bukan perangkat tiruan; dapat mengikat "satu manusia = satu perangkat" tanpa mengetahui identitasnya.	Pemeriksaan latar belakang terintegrasi dalam proses pendaftaran, tanpa memerlukan biometrik.	Membatasi bot farm; mengurangi pembuatan akun otomatis di aplikasi pengiriman pesan, media sosial, atau platform gim (game).
Berbasis interaksi/ tantangan	Pengguna menyelesaikan perintah yang menyerupai uji keaktifan atau tugas tantangan-respons kriptografi yang tidak dapat dilakukan oleh bot. Tidak ada data biometrik yang digunakan.	Tugas interaksi manusia yang sederhana (misalnya, gerakan terkontrol, perintah berwaktu), tetapi jauh kurang mengganggu dibandingkan CAPTCHA tradisional.	Berguna bagi platform media sosial dan komunitas daring untuk mencegah profil palsu tanpa memerlukan identitas atau biometrik.
Pengesahan sosial / jaringan kepercayaan	Pengguna diverifikasi oleh anggota komunitas tepercaya atau jaringan reputasi; platform mengubah ini menjadi sinyal PoH.	Dukungan atau konfirmasi secara ringkas dari pengguna/komunitas yang terverifikasi.	Lokapasar sejawat (peer-to-peer), platform pekerja lepas, atau lingkungan verifikasi berbasis komunitas.

Tabel 3.1: Bentuk Verifikasi Proof of Human (PoH)

Bagaimana ‘Proof of Human’ dapat membantu memerangi penipuan

Meskipun masih merupakan konsep baru, PoH berpotensi menjadi sangat relevan dalam memerangi penipuan dan kecurangan. Penipuan daring saat ini berskala besar: para pelaku kejahatan dan kelompok kriminal menciptakan ribuan akun palsu untuk memikat korban, mengotomatiskan penipuan pig-butchering, atau mengoperasikan jaringan rekening perantara yang menampung uang hasil kejahatan (money-mule accounts). Kemampuan untuk memproduksi persona digital secara murah dan massal menurunkan ongkos penipuan sekaligus melampaui kapasitas platform dan regulator untuk mendeteksi aktivitas kejahatan. Sebaliknya, PoH dapat membantu menggeser keseimbangan dengan memperkuat jaringan manusia otentik, membatasi penyebaran identitas palsu atau otomatis dalam skala besar.

Pada prinsipnya, PoH dapat memperkenalkan hambatan pada titik pembuatan akun atau transaksi, membatasi kecepatan dan skala penggandaan akun palsu.

Keberadaan manusia yang dapat diverifikasi dapat memiliki beberapa fungsi:

1. Mencegah profil palsu yang bertindak sebagai umpan dalam penipuan asmara, pekerjaan, atau investasi. Alih-alih mengandalkan penghapusan reaktif setelah korban sudah terperangkap, PoH dapat membantu mengurangi pasokan akun palsu sejak awal.

2. Melindungi sistem keuangan dengan mengurangi aliran transaksi melalui rekening perantara (mule-account). Bank dan jaringan pembayaran sering mengalami kesulitan membedakan antara pengguna yang sah dan akun palsu; sinyal sifat manusia yang dapat digunakan kembali dapat memperkuat perlindungan Know Your Customer (KYC) dan Anti Pencucian Uang (AML) yang ada tanpa memerlukan pengungkapan data pribadi secara terus-menerus.

3. Memperkuat kepercayaan dalam perdagangan digital dan komunitas daring. Di negara di mana penipuan dan peniruan identitas telah mengikis kepercayaan, kemampuan untuk memverifikasi bahwa pembeli, penjual, atau anggota komunitas adalah manusia sungguhan pada akhirnya dapat membantu memulihkan kepercayaan pada pertukaran langsung antar individu, platform kerja lepas, dan ruang sosial.

Pengamanan dan Tata Kelola

Pengamanan sangat penting untuk memastikan bahwa PoH itu sendiri tidak menjadi alat pengawasan. Berbagai model yang muncul menekankan desain yang menjaga privasi. Bukti kriptografi dan metode pembuktian tanpa pengetahuan/informasi penting (zero-knowledge) memungkinkan pengguna untuk menunjukkan dirinya adalah manusia tanpa menunjukkan data identitas yang mendasarinya. Perbedaan antara verifikasi identitas (apakah pelakunya manusia?) dan pengungkapan identitas (siapa pelakunya?) sangat penting untuk menjaga hak dan kepercayaan di berbagai yurisdiksi. Pengamanan juga membutuhkan tata kelola yang kuat: pengawasan oleh regulator, badan standar, atau audit multi-pemangku kepentingan dapat membantu mencegah sinyal PoH digunakan kembali untuk pelacakan atau pembuatan profil yang mengganggu.

Hak pengguna dan inklusi merupakan dua hal yang sama pentingnya. Verifikasi harus bersifat sukarela, transparan, dan dapat dibatalkan, di mana individu dapat memahami dan mengontrol bagaimana sinyal PoH mereka digunakan. Alat pelengkap seperti mekanisme penjaminan usia dapat melindungi anak di bawah umur tanpa memerlukan pengungkapan informasi sensitif, sementara berbagai jalur verifikasi membantu menghindari pengucilan orang-orang yang tidak mempunyai ponsel pintar, biometrik, atau konektivitas yang stabil. Kredibilitas PoH pada akhirnya akan bergantung pada apakah metode ini dapat meningkatkan keamanan sambil menghormati privasi, memastikan aksesibilitas, dan selaras dengan komitmen regional terhadap kepercayaan digital.

Namun, pengamanan teknis saja tidak cukup. Penerapan PoH yang efektif membutuhkan struktur tata kelola yang mencerminkan realitas ekosistem digital di Asia Pasifik. Sistem identitas digital nasional beroperasi di bawah aturan domestik, sementara sebagian besar interaksi pengguna sebenarnya—dan sebagian besar risiko yang sensitif terhadap privasi—terjadi di platform global. Karena kesenjangan struktural ini, integrasi langsung antara pemerintah dan platform jarang dapat dilakukan dengan sendirinya. Sebuah lapisan tata kelola netral sering kali dibutuhkan: perantara interoperabilitas independen yang dapat menerjemahkan persyaratan, mengumpulkan pemangku kepentingan, dan mendukung pengujian yang aman sebelum diadopsi dalam skala besar.

Perantara semacam itu dapat membantu memastikan bahwa PoH diimplementasikan dengan cara yang realistis secara teknis, menghormati privasi, dan selaras dengan kerangka kerja nasional serta lingkungan lintas platform. Mereka dapat menerjemahkan standar domestik menjadi panduan operasional, menyelenggarakan diskusi multi-pemangku kepentingan tentang privasi dan auditabilitas, serta memfasilitasi lingkungan ruang uji coba (sandbox) yang memungkinkan PoH diujicobakan dengan aman tanpa risiko yang tidak diinginkan bagi pengguna atau platform.

Pengamanan lebih lanjut berkaitan dengan kepercayaan publik. PoH adalah konsep baru—yang berbeda dari identitas digital, otentikasi, atau eKYC—dan kesalahpahaman dapat dengan mudah menimbulkan kekhawatiran tentang pengawasan atau penggunaan data. Inilah mengapa peningkatan kapasitas sama pentingnya dengan teknologi itu sendiri. Perantara netral, kelompok industri, dan jaringan masyarakat sipil dapat membantu menjelaskan cara kerja desain yang menjaga privasi, yang memperkuat bahwa PoH menjawab pertanyaan "Apakah Anda manusia?" tanpa mengungkapkan "Siapakah anda?", dan menawarkan panduan praktis bagi implementasi yang bertanggung jawab. Komunikasi yang kuat dan edukasi pengguna pada akhirnya adalah hal yang menerjemahkan sistem PoH yang dirancang dengan baik menjadi sesuatu yang membuat orang merasa nyaman untuk mengadopsinya.

Terakhir, PoH harus tertanam dalam kerangka kepercayaan dan keamanan. Memverifikasi bahwa pengguna adalah manusia tidak menjamin bahwa niat pengguna baik. Banyak penipuan paling berbahaya di Asia Pasifik—seperti penipuan investasi, penipuan peniruan identitas, dan skema rekayasa sosial jangka panjang— yang dilakukan oleh operator manusia sungguhan. Karena itulah mengapa PoH harus melengkapi, bukan menggantikan, sinyal keamanan lainnya. Menerapkan kerangka kerja seperti ISO/IEC 25389 (Kerangka Kerja Aman/The Safe Framework) membantu memastikan bahwa PoH digunakan dengan tepat:

- sebagai pertahanan berlapis terhadap otomatisasi dan serangan skala besar;
- bersamaan dengan sinyal perilaku dan reputasi yang mendeteksi ancaman yang digerakkan oleh manusia;
- dengan panduan implementasi yang jelas untuk menghindari ketergantungan yang berlebihan.

Oleh karena itu, PoH harus diujicobakan sebagai inovasi pelengkap, bukan pengganti, untuk memperkuat kerangka identitas yang sudah ada. Jika dirancang dan diatur dengan cermat, PoH dapat membantu menguji cara-cara baru untuk memverifikasi pengguna sebenarnya di lingkungan digital yang berisiko tinggi, yang dapat memberikan bukti tentang apa yang mungkin berhasil dalam skala yang lebih besar. Secara lebih luas, kerangka kerja PoH yang interoperabel dan menghormati hak manusia dapat melengkapi inisiatif identitas digital nasional, mendukung pengakuan lintas batas, dan memberikan dasar kepercayaan baru untuk kerja sama regional dalam hal mengatasi penipuan dan kecurangan di seluruh kawasan Asia Pasifik— sehingga dapat membantu negara-negara membangun jaringan manusia yang tangguh dan dapat diverifikasi yang mampu menahan skala dan kecepatan kejahatan daring modern.

Bagian selanjutnya akan membahas pengalaman di tingkat negara di Asia Pasifik PAC untuk mempertimbangkan bagaimana PoH dapat dilaksanakan.

Studi Kasus: Teknologi Canggih dalam Praktik

Di seluruh Asia, pemerintah telah membangun fondasi identitas digital yang kuat yang memverifikasi warga negara untuk layanan publik dan keuangan. Namun, sebagian besar penipuan terjadi di luar sistem yang diregulasi ini— seperti di platform media sosial, platform pengiriman pesanan, dan konten di mana anonimitas berlaku. Teknologi Proof of Human (PoH) yang sedang berkembang menawarkan sebuah cara untuk memperluas keandalan identitas digital ke lingkungan terbuka ini, mengonfirmasi manusia (humanness) dan keunikan tanpa mengungkapkan data pribadi. Studi kasus berikut meneliti bagaimana empat negara—Jepang, Korea Selatan, Malaysia, dan Filipina—membangun elemen verifikasi seperti PoH melalui sistem nasional mereka, dan pelajaran apa yang dapat dipetik dari pengalaman mereka untuk strategi ketahanan terhadap penipuan di masa depan.

Jepang: Sistem My Number dan Tantangan Kepercayaan

Sistem My Number Jepang, yang diluncurkan pada tahun 2016, memberikan pengidentifikasi unik 12 digit kepada setiap penduduk untuk keperluan perpajakan, jaminan sosial, dan penanggulangan bencana.[20] Sistem ini bertujuan untuk menyatukan data administratif dan meningkatkan efisiensi, dan telah berkembang ke ranah digital melalui Kartu My Number—sebuah kartu identitas pintar yang memungkinkan otentikasi daring yang aman untuk layanan e-government, layanan kesehatan, dan transaksi keuangan.[21] Pada tahun 2025, lebih dari 90 juta kartu—mencakup lebih dari 70 persen populasi—telah diterbitkan, meskipun penggunaan digital masih terbatas karena integrasi layanan yang tidak merata dan masalah kepercayaan yang terus berlanjut.[22]

Meskipun My Number memberikan keunikan yang diverifikasi dalam skala nasional, sistem ini tetap merupakan sistem identitas tradisional, bukan kerangka kerja Proof of Human (PoH). Verifikasi didasarkan pada registrasi pemerintah dan validasi dokumen, tanpa jaminan privasi atau kriptografi yang menjadi ciri khas teknologi PoH. Meskipun demikian, pengalaman Jepang menunjukkan bagaimana verifikasi keunikan yang didukung negara dapat berfungsi sebagai landasan untuk memperluas kepercayaan digital dan pencegahan penipuan—jika dipadukan dengan mekanisme modern yang meningkatkan privasi.

Pada saat yang sama, perjalanan pengalaman Jepang menunjukkan keterbatasan sistem identitas terpusat dalam memerangi penipuan. Sebagian besar penipuan dan peniruan identitas daring terjadi di lingkungan yang kurang diregulasi, seperti media sosial, layanan pesan, dan perdagangan elektronik (e-commerce). Berbagai platform ini beroperasi dalam kerangka peraturan konsumen dan konten umum, tetapi tetap berada di luar mekanisme jaminan yang terkait identitas di Jepang. Sementara itu, insiden penanganan data seperti kesalahan catatan asuransi kesehatan tahun 2023 telah mengikis kepercayaan publik dan menghidupkan kembali perdebatan tentang privasi, pengawasan, dan akuntabilitas.[23] Beberapa contoh ini menunjukkan bahwa kepercayaan, bukan teknologi, tetap menjadi kendala utama dalam memperluas penggunaan identitas terverifikasi. Budaya privasi Jepang—yang dibentuk oleh norma-norma yang kuat seputar anonimitas dan sikap hati-hati terhadap penanganan data negara—menjadikan penerimaan sosial sebagai faktor penting dalam menerapkan mekanisme verifikasi baru seperti PoH.

Sebagai tanggapan, pemerintah telah memperkenalkan langkah-langkah tata kelola dan interoperabilitas yang lebih kuat, sebagai upaya memperluas otentikasi berbasis Kartu My Number (JPKI) ke domain sektor swasta, seperti perbankan, pendaftaran SIM, dan perdagangan online. [24] Jika diimplementasikan secara transparan, Jepang dapat mengembangkan sistemnya menjadi model kepercayaan digital campuran (hybrid) — yang menambatkan identitas legal pada verifikasi negara sembari mengizinkan bukti keunikan ala PoH melalui metode kriptografi yang menjaga privasi. Evolusi ini akan memungkinkan Jepang untuk menghubungkan identitas terpercaya dengan verifikasi yang meningkat skalanya tanpa menurunkan kualitas dan menghormati privasi, sehingga memperkuat ketahanan terhadap penipuan dan kepercayaan publik pada ekonomi digital.[25]

Korea Selatan: Integrasi Identitas Digital dan Verifikasi Nama Asli (Real-Name Verification)

Korea Selatan mengoperasikan salah satu ekosistem identitas digital paling canggih dan terintegrasi di dunia, yang dibangun di sekitar infrastruktur identitas elektronik (e-ID) nasional yang menghubungkan layanan perbankan, telekomunikasi, dan e-government.[26] Berawal dari sistem Nomor Registrasi Penduduk (RRN) yang diperkenalkan pada tahun 1968, kerangka identitas Korea telah berevolusi melalui berbagai lapisan verifikasi nama asli, otentikasi biometrik, dan infrastruktur kunci publik untuk mendukung ekonomi daringnya yang berkembang pesat.[27] Kartu Identitas Digital (2020) dan Surat Izin Mengemudi Digital (2022) menandai tonggak penting dalam transisi dari kertas ke kredensial yang sepenuhnya digital.[28] Pada tahun 2025, lebih dari 50 juta warga Korea menggunakan otentikasi digital setiap hari—melalui PASS, Kakao, Naver, atau Samsung Pass—untuk mengakses layanan keuangan, pemerintah, dan sektor swasta.[29]

Integrasi identitas yang mendalam di berbagai platform ini telah menjadi inti dari rezim nama asli dan keamanan siber Korea, yang mengharuskan individu untuk memverifikasi identitas legal mereka dalam transaksi daring. Mekanisme ini berfungsi sebagai lapisan Proof of Human/PoH de facto, yang memastikan bahwa pelaku digital sesuai dengan individu nyata dan unik, serta mengurangi penipuan, identitas palsu, dan penyalahgunaan otomatis secara signifikan. Interoperabilitas antara sistem publik dan swasta telah menghasilkan tingkat kepercayaan yang tinggi dan tercatat memiliki tingkat penipuan identitas keuangan terendah di dunia.[30]

Namun, model Korea juga mengungkapkan konsekuensi dari sentralisasi yang kuat. Aturan wajib penggunaan nama asli dan berbagi data antar entitas telekomunikasi, keuangan, dan pemerintah telah menimbulkan kekhawatiran tentang privasi dan kebebasan sipil. Pelanggaran data skala besar, termasuk kebocoran dari biro kredit dan platform e-commerce, telah meningkatkan skeptisisme publik tentang persetujuan (consent) dan minimalisasi data.[31] Sebagai respons, para pembuat kebijakan telah memperkuat perlindungan berdasarkan Undang-Undang Perlindungan Informasi Pribadi (Personal Information Protection Act/PIPA) dan meluncurkan Proyek Percontohan Identitas Digital (2023) yang mengeksplorasi otentikasi terdesentralisasi yang dikendalikan pengguna—sebuah langkah penting menuju model yang lebih menjaga privasi.[32]

Pengalaman Korea menunjukkan kekuatan sekaligus keterbatasan sistem PoH yang didukung negara. Kombinasi identitas legal yang terverifikasi, jaminan biometrik, dan kerangka kepercayaan yang selaras/kompatibel (interoperable) menawarkan pola dasar (template) yang ampuh untuk pencegahan penipuan dan kepercayaan digital. Namun, perdebatan di Korea juga menyoroti meningkatnya minat pada pendekatan yang menawarkan privasi dan kontrol pengguna yang lebih kuat—prinsip-prinsip yang selaras dengan arah teknologi Proof of Human (PoH) yang sedang berkembang. Seiring Korea menyempurnakan arsitektur kepercayaan digitalnya, perkembangan di masa depan mungkin akan kurang fokus pada mekanisme penggunaan nama asli yang ketat dan lebih banyak pada model yang seimbang yang memverifikasi pengguna sebenarnya sembari mempertahankan hak individu dan kepercayaan dalam ekonomi digital.

Malaysia: MyDigital ID dan Jalan Menuju Kepercayaan Biometrik

Inisiatif MyDigital ID Malaysia menandai langkah besar menuju kerangka identitas digital terpadu yang didukung negara, yang bertujuan untuk menyederhanakan akses ke layanan publik dan swasta. Diluncurkan pada tahun 2024 di bawah Cetak Biru Identitas Digital, sistem ini memberikan kredensial digital kepada setiap penduduk yang terhubung dengan biometrik dan terikat pada database Departemen Registrasi Nasional (National Registration Department/NRD).[33] Dengan menggunakan pengenalan wajah dan otentikasi yang aman, sistem ini memungkinkan individu untuk memverifikasi identitas mereka di berbagai portal e-government, bank, operator telekomunikasi, dan layanan daring lainnya. Uji coba awal dengan Lembaga Pendapatan Dalam Negeri (LHDN) /Inland Revenue Board dan lembaga keuangan terpilih menjadi dasar untuk peluncuran nasional penuh yang diharapkan terjadi pada tahun 2025.[34]

Berbeda dengan sistem ID sebelumnya, MyDigital ID dirancang untuk berfungsi sebagai lapisan kredensial dan verifikasi yang memungkinkan otentikasi tanpa berulang kali mengungkapkan detail pribadi. Dengan berlandaskan pada identitas dalam catatan biometrik yang terverifikasi, sistem ini memberikan landasan untuk verifikasi bergaya Proof of Human (PoH)— yang memastikan bahwa setiap akun digital sesuai dengan individu yang nyata dan unik. Seiring dengan perluasan verifikasi digital di berbagai sektor di Malaysia, negara ini menghadapi tantangan yang sama seperti negara-negara lain: memperluas kepercayaan terhadap ekosistem terbuka yang digerakkan oleh pengguna, di mana pengungkapan identitas penuh tidak praktis dan tidak diinginkan. Dalam hal ini, MyDigital ID dapat berfungsi sebagai tulang punggung untuk mekanisme PoH di masa depan yang memverifikasi manusia dengan tetap menjaga privasi dan memastikan interoperabilitas.

Inisiatif ini juga secara langsung merespons meningkatnya paparan Malaysia terhadap penipuan dan kecurangan digital, seiring dengan adopsi perbankan seluler (mobile banking) dan perdagangan elektronik (e-commerce). Lapisan identitas terpercaya dapat membantu mengurangi peniruan identitas dan akun palsu dalam ekosistem yang teregulasi, sementara verifikasi ala PoH pada akhirnya dapat memperluas perlindungan ini ke ruang yang tidak diregulasi—seperti lokapasar (market place), media sosial, dan pembayaran digital—di mana penipuan sering kali berasal.

Namun, peluncuran tersebut telah memicu perdebatan publik mengenai privasi, perlindungan data, dan tata kelola. Kelompok masyarakat sipil telah menyuarakan kekhawatiran tentang penyimpanan biometrik terpusat dan potensi penyalahgunaan jika akses data diperluas melampaui tujuan yang dimaksudkan.[35] Sebagai tanggapan, pemerintah telah membentuk Komite Pengarah Identitas Digital, yang menegaskan kembali kepatuhan terhadap Undang-Undang Perlindungan Data Pribadi (Personal Data Protection Act /PDPA), dan menekankan interoperabilitas dengan sistem MySejahtera dan eKYC di bawah pengawasan Bank Negara Malaysia. Berbagai langkah ini bertujuan untuk memastikan bahwa implementasi berjalan secara transparan, akuntabel, dan mendapat kepercayaan publik.

Jika diimplementasikan dengan pengamanan yang jelas dan kontrol pengguna, MyDigital ID dapat berkembang menjadi fondasi identitas tepercaya untuk inovasi PoH. Arsitekturnya— yang menggabungkan biometrik terverifikasi, persetujuan pengguna, dan interoperabilitas yang aman—menggambarkan bagaimana negara-negara berkembang dapat menanamkan keunikan dan inklusivitas yang terverifikasi ke dalam kerangka kepercayaan digital. Bagi Asia Tenggara, pengalaman Malaysia menunjukkan bagaimana pengembangan identitas yang dipimpin oleh tata kelola dapat menjembatani kesenjangan antara sistem identitas digital tradisional dan model PoH masa depan, yang memperkuat ketahanan terhadap penipuan sambil menjaga privasi dan kepercayaan publik.

Filipina: Peluncuran Cepat PhilSys

Philippine Identification System (PhilSys) telah menjadi salah satu inisiatif identitas digital yang berkembang paling pesat di Asia Tenggara. Sistem ini dibuat berdasarkan Undang-Undang Republik No. 11055 tahun 2018, yang memberikan setiap warga negara dan penduduk nomor PhilSys (PSN) unik 12 digit yang didukung oleh data biometrik—termasuk pemindaian wajah, sidik jari, dan iris mata.[36] Program yang dikelola oleh Philippine Statistics Authority (Otoritas Statistik Filipina/PSA) bertujuan untuk meningkatkan akses ke layanan publik, mempromosikan inklusi keuangan, dan mengamankan transaksi digital. Pada akhir tahun 2025, lebih dari 80 juta warga Filipina telah terdaftar, dan versi digital dari sistem tersebut— tersedia melalui aplikasi eGovPH dan national-id.gov.ph—dan telah diterima di berbagai lembaga pemerintah, bank, dan platform swasta.[37]

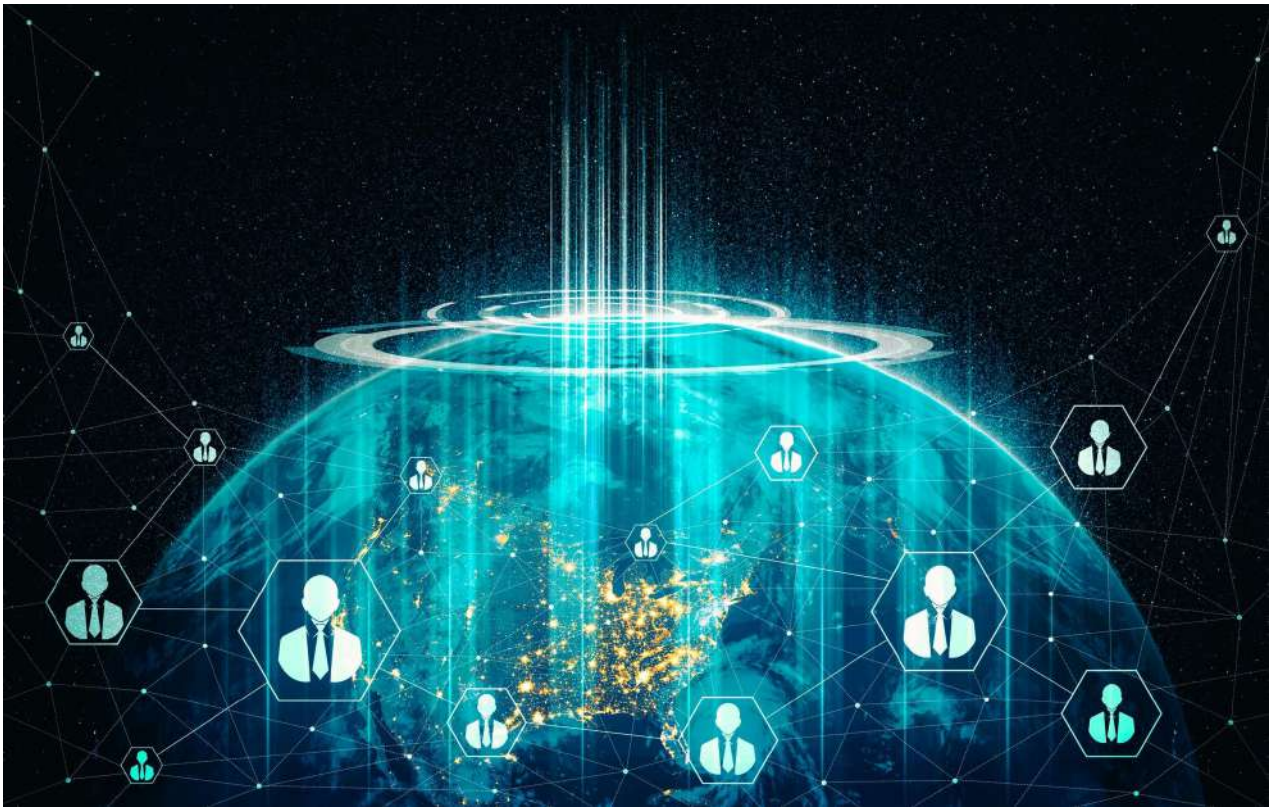
Peluncuran cepat ini merupakan langkah penting dalam upaya kawasan ini untuk mewujudkan identitas yang terpercaya. Dengan menghubungkan biometrik yang terverifikasi dengan pengidentifikasi unik dan permanen, PhilSys secara efektif menciptakan lapisan bukti keunikan yang didukung oleh negara, mencegah pendaftaran ganda dan identitas palsu. Integrasinya dengan lembaga keuangan, operator telekomunikasi, dan sistem pemerintah berfungsi sebagai analog skala besar awal untuk Proof of Human/PoH —yang memastikan bahwa setiap pengguna yang terverifikasi sesuai dengan individu yang nyata dan unik. Portal eVerify, yang memungkinkan verifikasi kredensial berbasis kode respons cepat (QR code) secara waktu nyata langsung (real-time), memperluas jaminan ini ke pembayaran digital, perlindungan sosial, dan pendaftaran SIM.[38]

Pada saat yang sama, kecepatan penerapan telah menimbulkan tantangan yang baru dalam tata kelola dan privasi. Kesalahan teknis, keterlambatan produksi kartu, dan masalah penanganan data telah menarik perhatian publik, sementara kekhawatiran mengenai penyimpanan biometrik terpusat dan berbagi data yang tidak transparan telah mendorong seruan untuk pengamanan yang lebih kuat.[39] PSA dan Komisi Privasi Nasional (National Privacy Commission / NPC) telah menanggapi hal ini dengan meningkatkan pengawasan, mengadopsi standar enkripsi yang lebih ketat, dan menyematkan protokol akses berbasis persetujuan (consent) dalam kerangka kerja eGovPH.[40]

Pengalaman Filipina menggambarkan potensi maupun risiko perluasan kepercayaan digital yang cepat. Skala dan interoperabilitasnya menunjukkan bagaimana ekonomi negara berkembang dapat melompat ke infrastruktur identitas terverifikasi yang mendukung inklusi keuangan dan pengurangan penipuan. Namun, peluncurannya juga menggarisbawahi bahwa kepercayaan harus berkembang seiring dengan teknologi: kepercayaan publik bergantung pada akuntabilitas yang terlihat, tata kelola data yang transparan, dan kendali pengguna. Seiring perkembangan PhilSys, sistem ini menawarkan tapak uji (testbed) yang berharga untuk inovasi yang selaras dengan PoH— yang menunjukkan bagaimana keunikan yang terverifikasi, jika dipadukan dengan perlindungan privasi dan inklusi yang kuat, dapat memperkuat ketahanan terhadap penipuan dan memastikan sistem yang berbasiskan kepercayaan manusia di sektor ekonomi digital Asia Tenggara.

Kesimpulan Studi Kasus

Keempat studi kasus ini secara bersama-sama menggambarkan perbedaan pendekatan yang ditempuh beberapa negara di Asia dalam membangun infrastruktur bukti keunikan. Jepang dan Korea Selatan menunjukkan bagaimana lingkungan regulasi yang maju dapat melembagakan identitas terverifikasi dalam skala besar, meskipun dengan hasil yang kontras: sistem My Number Jepang menunjukkan kerapuhan kepercayaan publik ketika tata kelola data goyah, sementara rezim Real-Name Korea menyoroti efisiensi—dan risiko—integrasi mendalam antara identitas, keuangan, dan teknologi. Di Asia Tenggara, MyDigital ID Malaysia dan PhilSys Filipina mengungkapkan dua model: yang satu menekankan tata kelola yang cermat sejak tahap perancangan, yang lain memprioritaskan peluncuran dan akses yang cepat. Dari keempatnya, muncul pola umum—verifikasi seperti PoH paling efektif bila dipadukan dengan transparansi, interoperabilitas, dan kontrol pengguna, yang dapat memastikan bahwa sistem identitas digital memperkuat, bukan mengikis, kepercayaan publik terhadap keamanan daring.



Kesimpulan dan Rekomendasi

Penipuan dan kejahatan daring telah menjadi ancaman utama bagi kepercayaan digital di seluruh kawasan Asia-Pasifik. Meskipun sistem identitas digital nasional—dari My Number Jepang hingga PhilSys Filipina—telah memajukan tujuan identitas yang terverifikasi dan inklusif, sistem tersebut utamanya tetap sebagai alat administratif daripada instrumen pencegahan penipuan secara waktu nyata langsung (real-time). Teknologi PoH yang sedang berkembang menawarkan lapisan pelengkap penting bagi sistem ini: memungkinkan individu untuk membuktikan bahwa mereka adalah pengguna manusia yang unik—tanpa mengungkapkan identitas pribadi—di seluruh platform digital, layanan keuangan, dan jaringan komunikasi. Dengan menambahkan bukti sebagai manusia yang menjaga privasi, PoH dapat mengatasi berbagai bentuk penyalahgunaan otomatis dan berskala besar yang tidak terdeteksi oleh sistem identitas digital tradisional. Oleh karena itu, mengintegrasikan PoH ke dalam ekosistem identitas digital dapat meningkatkan ketahanan terhadap penipuan dan kepercayaan publik terhadap transaksi digital, sambil tetap menjaga perlindungan privasi yang kuat.

Sebagaimana disoroti dalam bagian Perlindungan dan Tata Kelola, penerapan PoH yang bertanggung jawab memerlukan desain berbasis risiko, perlindungan pengguna yang jelas, dan penyelarasan yang cermat dengan ekosistem identitas yang ada. Berdasarkan prinsip-prinsip ini, pemerintah di kawasan ini dapat:

- **Integrate digital ID and PoH technologies into scam-prevention strategies:** Memasukkan verifikasi bukti keunikan ke dalam platform keuangan, perdagangan elektronik (e-commerce), dan komunikasi untuk mengurangi risiko peniruan identitas, penipuan yang digerakkan oleh bot, dan identitas palsu, dengan tetap memastikan penerapannya tetap proporsional, mudah, dan selaras dengan kerangka kerja keamanan seperti ISO/IEC 25389.

- **Mendukung standar yang menjaga privasi dan selaras (interoparable):** Mendorong pengembangan kerangka kerja regional yang menggabungkan jaminan biometrik dengan perlindungan privasi kriptografi, memastikan bahwa keunikan yang terverifikasi tidak mengganggu anonimitas pengguna atau kegunaan lintas batas, dan bahwa sinyal PoH tidak dapat digunakan kembali untuk pelacakan atau pemprofilan.

- **Mendorong dialog dan koordinasi kebijakan regional:** Memanfaatkan mekanisme yang ada seperti APEC Business Advisory Council, G20 High-Level Principles for Digital Financial Inclusion, dan inisiatif ekonomi digital yang dipimpin PBB untuk menyelaraskan tujuan kebijakan, berbagi praktik terbaik, dan mengeksplorasi kerangka kerja percontohan untuk verifikasi berbasis PoH di berbagai sektor, termasuk lingkungan uji coba terkendali yang memungkinkan pemerintah dan platform untuk menguji PoH di lingkungan berisiko tinggi sebelum diadopsi secara lebih luas

Berbagai langkah ini bersama-sama akan membantu membangun ekosistem digital yang lebih tepercaya dan berpusat pada manusia di Asia—ekosistem di mana verifikasi memperkuat keamanan tanpa mengikis privasi, di mana perlindungan dan kerangka kerja tata kelola memastikan penggunaan yang bertanggung jawab, dan di mana kolaborasi regional mengubah sistem identitas dari registrasi administratif menjadi perangkat yang aktif untuk ketahanan terhadap penipuan dan inklusi digital.

Bibliography

[1] Cybersecurity Ventures. n.d. “The World’s Third Largest Economy Has Bad Intentions—And It’s Only Getting Bigger.” Diakses Agustus 2025. https://cybersecurityventures.com/the-worlds-third-largest-economy-has-bad-intentions-and-its-only-getting-bigger/.
[2] Feedzai. 2024. “GASA Global State of Scams Report: $1T Lost to Scams.” Diakses Agustus 2025. https://www.feedzai.com/blog/gasa-global-state-of-scams-report-1t-lost-to-scams/.
[3] GSMA. 2025. Fraud and Scams Safety Report. London: GSMA. https://www.gsma.com/solutions-and-impact/connectivity-for-good/public-policy/wp-content/uploads/2025/02/Fraud-and-scams-safety-report.pdf.
[4] UNODC, Inflection Point: Global Implications of Scam Centres (2025), p. xx, https://www.unodc.org/roseap/uploads/documents/Publications/2025/Inflection_Point_2025.pdf
5 Global Initiative, CRIME CYBER SCAM OPERATIONS IN SOUTHEAST ASIA (May 2025), https://globalinitiative.net/wp-content/uploads/2025/05/GI-TOC-Compound-crime-Cyber-scam-operations-in-Southeast-Asia-May-2025.pdf
[6] “A New Human Trafficking Trend Emerges from Myanmar,” The Japan Times, April 2, 2025, https://www.japantimes.co.jp/news/2025/04/02/japan/crime-legal/myanmar-scam-human-trafficking/
[7] “They were forced to scam others worldwide. Now thousands are detained on the Myanmar border,” AP News, 9 Maret, 2025, https://apnews.com/article/myanmar-thailand-scam-centers-trapped-humanitarian-c1cab4785e14f07859ed-59c821a72bd2
[8] Signicat. 2024. “Fraud Attempts with Deepfakes Have Increased by 2137% over the Last Three Years.” Diakses Agustus 2025. https://www.signicat.com/press-releases/fraud-attempts-with-deepfakes-have-increased-by-2137-over-the-last-three-year.
[9] CSIS, Cyber Scamming Goes Global: Unveiling Southeast Asia’s High-Tech Fraud Factories, Desember 12, 2024, https://www.csis.org/analysis/cyber-scamming-goes-global-unveiling-southeast-asias-high-tech-fraud-factories
[10] TRM Labs, The Illicit Crypto Ecosystem Report (2022), https://www.trmlabs.com/resources/reports/the-illicit-crypto-ecosystem-report-2022.
[11] Meta, “Cracking Down on Organized Crime Behind Scam Centers,” November 21, 2024, https://about.fb.com/news/2024/11/cracking-down-organized-crime-scam-centers/
[12] TRM Labs, 2025 Crypto Crime Report, https://www.trmlabs.com/reports-and-whitepapers/2025-crypto-crime-report
[13] World Bank, Digital Identity Toolkit (World Bank), section on credential and smart cardbased eIDs. https://documents1.worldbank.org/curated/en/147961468203357928/pdf/912490WP0Digit00Box385330B00PUBLIC0.pdf
[14] Financial Action Task Force (FATF), Guidance on Digital Identity (Paris: FATF/OECD, Maret 2020), https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-on-Digital-Identity.pdf (discussion of biometric authentication as part of digital ID assurance).
[15] SITA and PRISM, Biometric Digital Identity: The Next Step in Seamless Travel and Government Services (2023), https://www.sita.aero/globalassets/docs/other/biometric-digital-identity-govt-services-prism-report.pdf
[16] OECD, National Digital Identity (NDID) Platform (Thailand), https://www.oecd.org/content/dam/oecd/en/topics/policy-issues/tax-administration/thailand-national-digital-identity-platform.pdf
[17] “Digital Identity Spotlight: Singapore,” 1Kosmos, https://www.1kosmos.com/identity-management/digital-identity-spotlight-singapore/
[18] “Digital identity systems around Asia compared as Taiwan seeks path forward,” BiometricUpdate, https://www.biometricupdate.com/202102/digital-identity-systems-around-asia-compared-as-taiwan-seeks-path-forward
[19] Kleros, Proof of Humanity (PoH) Documentation, “Proof of Humanity (PoH) is a sybil-resistant registry of humans, combining social verification with video submission to create a trusted list of real humans,” https://docs.kleros.io/products/proof-of-humanity
[20] Government of Japan, Cabinet Office, “Outline of the Social Security and Tax Number System (My Number System),” 2016, https://www.cao.go.jp/bangouseido/english/.
[21] Ministry of Internal Affairs and Communications (MIC), “Overview of the Social Security and Tax Number System,” diperbaharui 2024.
[22] Digital Agency of Japan, My Number Card Statistics Portal, “Number of My Number Cards Issued,” updated October 2025; “Japan’s My Number cards hit 90m issuance but trust issues persist,” Nikkei Asia, 12 Juli 2025.
[23] “Japan suspends some My Number links after health-insurance data mix-up,” Reuters, 28 Mei 2023
[24] “Japan aims to link My Number to banking and SIM registration,” Japan Times, 9 Maret 2024.
[25] “Fix the flaws in the My Number system,” Japan Times (editorial), 2 Juni 2023; Digital Agency, “Efforts to Enhance Trust in the My Number System,” 2024.

[26] Ministry of the Interior and Safety (MOIS), “Overview of the Resident Registration System,” Government of the Republic of Korea, 2023.
[27] Korea Communications Commission (KCC), Real-Name Verification Policy in the Digital Environment, 2022.
[28] Ministry of Land, Infrastructure and Transport (MOLIT), “Launch of the Mobile Driver’s License Service,” press release, Januari 2022.
[29] Korea Internet & Security Agency (KISA), “Status of Digital Authentication Use in Korea,” 2024; Yonhap News, “PASS App Surpasses 50 Million Users in Korea,” 9 Mei 2025.
[30] OECD, Digital Government in Korea: Enabling a Smart and Inclusive Society, 2023, p. 45.
[31] Korea JoongAng Daily, “Massive Data Leaks Raise Questions About Security Practices,” 4 Februari 2023; Korea Times, “Credit Bureau Fined over Data Breach Affecting Millions,” 15 April 2023.
[32] MOIS, “Digital Identity Pilot Project for Secure Authentication,” 2023; Personal Information Protection Commission (PIPC), “Amendments to the Personal Information Protection Act,” Desember 2023.
[33] Malaysia Digital Economy Blueprint (MyDIGITAL), Digital Government Division, Ministry of Communications and Digital, “Digital Identity Blueprint,” Government of Malaysia, 2024.
[34] Department of National Registration (Jabatan Pendaftaran Negara, JPN), “Implementation of MyDigital ID Pilot with LHDN and Financial Institutions,” press release, Juni 2024.
[35] Malay Mail, “Privacy Advocates Raise Concerns over Centralised Biometric Database,” 5 April 2024.
[36] Republic Act No. 11055, “An Act Establishing the Philippine Identification System (PhilSys Act),” Official Gazette of the Republic of the Philippines, Agustus 2018.
[37] Philippine Statistics Authority (PSA), PhilSys Dashboard: Registration and Issuance Data, updated October 2025; Inquirer.net, “Over 80 Million Filipinos Registered for National ID—PSA,” 14 September 2025.
[38] PSA, “PhilSys eVerify Portal Launch and QR Verification Capabilities,” 2024.
[39] Rappler, “Privacy Concerns Mount over National ID Data Sharing,” 22 Juni 2024; Philippine Star, “National ID Delays, Data Glitches Spur Criticism,” 10 Mei 2024.
[40] National Privacy Commission (NPC), “NPC Advisory on Data Protection Standards for the National ID System,” 2024; PSA, “Enhanced Security Measures for ePhilID Rollout,” 2024.