Digitális identitáskezelés átalakulóban: önrendelkezésű identitások

KOCSIS IMRE
BME Méréstechnika és Információs Rendszerek Tanszék
kocsis.imre@vik.bme.hu

Kulcsszavak: önrendelkezésű identitás, decentralizált identitás, ellenőrizhető tanúsítványok, EBSI, blokklánc

A folyamatosan növekvő összekötöttséggel és digitalizációval az online és digitális azonosítás klasszikus modelljei jó ideje egyre nehézkesebben alkalmazhatóak. A változást az önrendelkezésű identitások (Self-Sovereign Identity) jelenleg folyamatban lévő szabványosítása és bevezetése hozza el. A cikk áttekinti az SSI filozófiáját és legfőbb támogató W3C-szabványait az elosztott identitásokra és az ellenőrizhető tanúsítványokra. A cikk fontos használati eseteken keresztül demonstrálja az SSI alapvető működési modelljét, és bemutatja a legfontosabb, már ma is működő támogatóhálózatokat, ezek között a European Blockchain Service Initiative-t is, továbbá a megjelenőben lévő ipari használati esetek is röviden áttekintésre kerülnek.

1. Bevezetés

Világunk és életünk egyre inkább hálózatokhoz kötötté és „kiberfizikaibbá" válásával a digitális és online identitáskezelés klasszikus megközelítései egyre kevésbé képesek az azonosítás és tulajdonság-meghatározás biztonságos, hatékony és sok fél között interoperábilis támogatására. Az önrendelkezésű identitások – angol terminológiában Self-Sovereign Identity (SSI) – filozófiája, szabványai és technológiái hosszú idő óta formálódnak viszonylag szűk szakmai körökben; az utóbbi években azonban terjedésük széles körben is megindult az újszerű műszaki képességek és részben újszerű vállalati, szabályozói és állami igények egymásra találásával.

Cikkünk áttekintő bevezetést nyújt az önrendelkezésű identitások kialakulóban lévő szakterületére és szemlélteti a jelenlegi főbb megvalósításokat, azok alkalmazásaira is rámutatva. Kitérünk az Európai Unión belüli digitális azonosítás és az SSI kapcsolatára, végül rámutatunk az SSI – jelenleg még részben felderítés alatt álló – ipari és telekommunikációs relevanciájára.

A cikk következő szakasza az önrendelkezésű identitások filozófiáját és alapfogalmait mutatja be. A harmadik szakasz a jelenlegi szabványtámogatást ismerteti, majd a jelenleg rendelkezésre álló főbb platformokat és hálózatokat veszi sorra. Az ötödik szakasz az önrendelkezésű identitások tágabb európai kontextusát szemlézi, végül a megjelenőben lévő ipari alkalmazásokra mutat rá.

2. Önrendelkezésű identitások

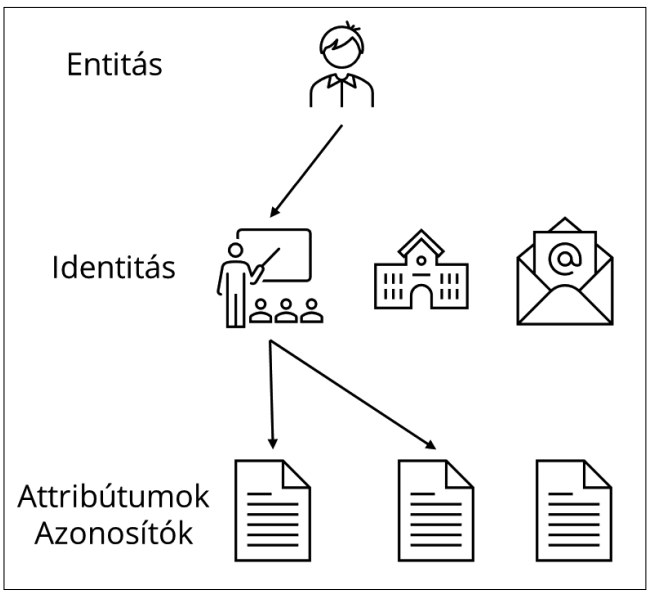
Általános értelmű fogalomként egy természetes személy identitása azt ragadja meg, hogy „ki ő"; mik azok a tulajdonságai, amik másoktól megkülönböztetik *(1. ábra)*.

A hétköznapi életben mindannyian számos identitással rendelkezünk: más-más jellemzőink relevánsak a munkahelyen, az állammal szemben és a magánéletben. Identitásunk részét képezik végzettségeink, a hivatalos személyazonosságunk, különböző jogosítványaink és felhatalmazásaink is. Ezek bizonyítására elfogadunk (visszavonható) „tanúsítványokat" különböző állami és nem állami forrásoktól, de az természetes igény marad, hogy az identitásainkkal magunk rendelkezhessünk és ne az identitásunkkal kapcsolatban tanúsítványokat kiállító felek.

2.1. Az online identitáskezelés klasszikus megközelítései

Ezt a természetes igényt ma nem elégítik ki sem az általános értelemben vett digitális azonosítás, sem pedig az online azonosítás széles körben elterjedt megoldásai, és ahogy életünk egyre inkább digitalizálttá válik, úgy egyre égetőbb kihívásként jelentkezik az identitások önrendelkezésűvé tételének megvalósítása.

1. ábra
A klasszikus identitásmodell: entitás, identitás, attribútumok



Az online világ meghatározó protokolljai, mint az IP és a TCP, a csomópontok és csomóponti szolgáltatások, és nem a felhasználók azonosítását támogatják – utóbbi nem is volt cél tervezésük során. Így azonban az internet egy, az alkalmazási réteg által is használható „bizalmi réteg" nélkül maradt.

Kezdetben az internetalapú alkalmazások külön-külön saját azonosítási megközelítéseket vezettek be – legtöbbünk mind a mai napig felhasználónév-jelszó párosok tucatjait kénytelen karbantartani. Ezen identitások felett azonban a szolgáltató rendelkezik; saját belátása szerint törölheti és módosíthatja őket. Érdemes megjegyeznünk, hogy mindez a szabványos, X.509 tanúsítvány alapú, jóval általánosabb használati körű digitális identitáskezelésre is igaz, – csak hierarchiába szervezett módon.

Emellett évtizedek óta probléma az is, hogy a szolgáltatótól az „identitás" ki is szivároghat, ezért is javasolt ragaszkodnunk az egyszer használatos jelszavakhoz. Végeredményben a klasszikus, centralizált modellben nagyszámú identitást hozunk létre az esetek többségében alapvetően egy cél érdekében; identitásazonosításra a szolgáltatás igénybevételéhez *(2. ábra)*.

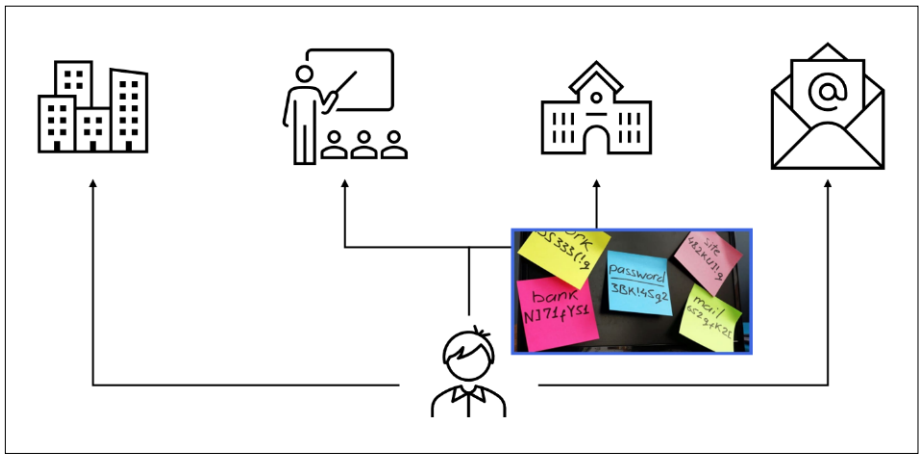
Ezt a töredezettséget próbálták a 2000-es években először néhány szervezetek közötti identitás-federációs megoldással, majd olyan „felhasználóközpontú" identitáskezelési sémákkal (pl. OpenID, OAuth) orvosolni, melyek felhasználói hozzájáruláshoz kötik az identitások szolgáltatások közötti megosztását. Végeredményben egy olyan online világ alakult ki – a technológiák teljes képességkészletétől függetlenül – ahol néhány nagy alkalmazásszolgáltató identitásszolgáltatás-federációt is végez. (Gondoljunk csak arra, hogy hány kisebb szolgáltatónál lehetséges a google-fiókunkkal vagy a facebook-fiókunkkal belépni *(3. ábra)*.

Bár így a töredezettség csökken és az identitások szolgáltatások közötti átjárhatósága nő, a végfelhasználó az identitáskezelés tekintetében még inkább kiszolgáltatottá válik egy olyan piaci (és nem állami) szereplő felé, amelyik ingyenes szolgáltatása felhasználási feltételeiben sokszor explicite nem vállal semmilyen érdemi garanciát.

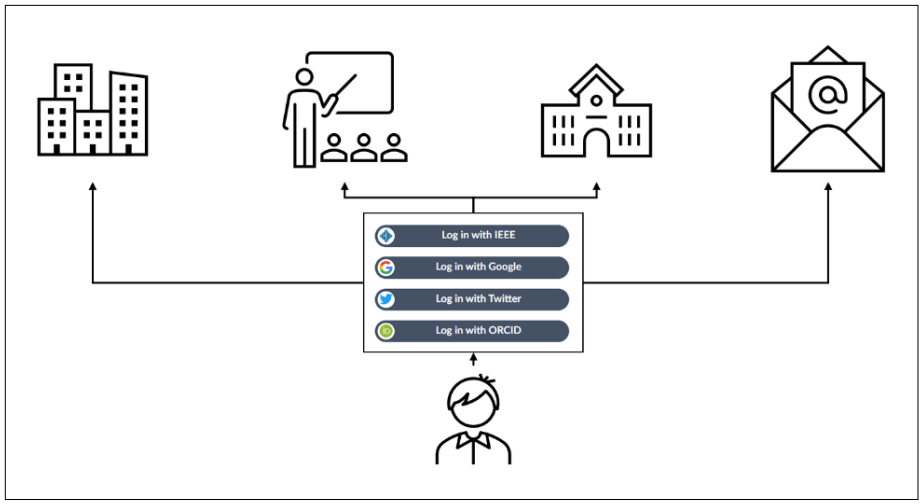
Mind a mai napig a centralizált és federált jellegű identitáskezelési megoldások jellemzik a széles körben alkalmazott digitális identitáskezelési megoldásokat (a hierarchikus tanúsítványkezelés mellett). Évek óta zajlik azonban a radikális változások előkészítése több terület összefogásával, amelyek között – az adatbiztonság identitáskezelés aldiszciplínája mellett – kiemelt szerepe van a blokklánc-technológiáknak és a közszférának is.

2.2. Az önrendelkezésű identitások jellemzői

A 2010-es évek közepén kezdtek körvonalazódni az „önrendelkezésű identitásokkal" kapcsolatos alapvető követelmények. Nagyhatású cikkében Christopher Allen



2. ábra
Klasszikus online identitáskezelés



3. ábra
Felhasználói hozzájárulással federált online identitáskezelés

kriptográfus ezeket tíz elvként definiálja [1], melyekből jelen cikk szerzője a következőket tartja a legfontosabbaknak:

– Kontroll – a felhasználó teljes mértékben rendelkezzen az identitásai felett.
– Hozzáférés – a felhasználó teljes mértékben férjen hozzá az identitásaival kapcsolatos adatokhoz.
– Perzisztencia – a felhasználó identitásai addig létezhessenek, ameddig csak a felhasználó azt szeretné (akár örökké).
– Interoperabilitás – az identitások széles körben használhatóak legyenek, geográfiailag és informatikailag is.
– Hozzájárulás – az identitás bármilyen használatához a felhasználó hozzájárulása legyen szükséges.
– Adatminimalizáció – az identitással kapcsolatos forgatókönyvekben legyen lehetőség csak a minimálisan szükséges információ közlésére.

2.3. A blokklánc-technológia hatása

Az SSI követelményeinek egyértelművé válásával párhuzamosan kialakultak és elterjedtek az üzemeltetés tekintetében szabad csatlakozású (unpermissioned) blokklánc-technológiák, mint a Bitcoin és az Ethereum [2], majd később a szervezetek jogosultságkezelt és diverz köre által üzemeltetett elosztott főkönyvön alapuló technológiai platformok (Distributed Ledger Technology, DLT) [3], mint amilyen például a Hyperledger Fabric [4]. A blokkláncok széles körű elterjedése az SSI szempontjából két alapvető elemmel gazdagította az informatikai rendszertervezés mintakészletét: a „többes hitelesítésű” adatregiszterekkel és az önrendelkezésű kriptográfiai azonosítással.

A blokkláncok koncepcionálisan „többes hitelesítésű” adatregiszterek: példájuk azt mutatja, hogy lehetséges létrehozni és hosszú távon sikeresen üzemeltetni olyan elosztott kvázi-adatbázisokat, ahol a módosítások befogadásáról az üzemeltető csomópontok valamilyen elégséges többsége dönt; a többség által az „adatbázis-protokoll” betartását vagy (kripto)pénzbeli ösztönző-mechanizmusok, vagy az üzemeltető közösség jogi megállapodásai szavatolják.

A blokklánc-technológiák felhasználói oldala hasonlóan fontos, a széles körű használat szempontjából új elem. A blokklánc-hálózattal szemben egy felhasználó a tranzakciók digitális aláírásával bizonyítja identitását. Ez az identitás azonban pusztán egy – a felhasználó által szabadon létrehozott aszimmetrikus kriptográfiai kulcspár publikus részéből levezethető – kriptográfiai álnév, melyhez a privát kulcsot az ún. „tárcájában” (wallet) tartja, mely egy hardveres vagy szoftveres megvalósítású céleszköz. A publikus blokklánc-hálózatokban egy adott publikus kulcsra (abból képzett „címre”) átvezetett kriptopénz csak a privát kulcs segítségével adható tovább az elosztott főkönyv által megvalósított könyvelésben. A felhasználó teljes mértékben maga rendelkezik a privát kulcshoz kötött identitása fölött a blokklánc-rendszerekben, és ezen identitásokból tetszőleges számút hozhat létre.

E két elemből származik a megjelenőben lévő SSI-szabványok és technológiai ökoszisztémák két alapgondolata: az identitások és a tanúsítványok erős szétcsatolása és a kriptográfiai alapú, önrendelkezésű identitáskezelés ellenőrizhető adatregiszterekben.

2.4. Decentralizált identitások

A centralizált és a legtöbb federált identitáskezelési megoldás alapvető gyengesége, hogy egységben kezeli az identitást – pontosabban: az identitás tulajdonlásának bizonyítását – és az identitásnak pusztán logikailag részét képező, időben változékony tanúsítványokat. Valójában ezek megfelelő kriptográfiai és adatregiszter-támogatással szétcsatolhatóak.

A séma egyik fele egy azonosító és az azonosító tulajdonlásának bizonyításához szükséges követelmények (tipikusan: publikus kulcs, aminek megfelelő digitális aláírást kell tudnia létrehozni), melyeket egy úgynevezett ellenőrizhető adatregiszterben (Verifiable Data Registry) tárolunk. Utóbbi lehet blokklánc, de akár centralizált, elégségesen megbízhatónak tartott – például állami üzemeltetésű – nyílt identitáskezelő szolgáltatás is. Ha az identitásokat decentralizált platformon kezeljük, akkor jellemzően decentralizált identitásként (decentralized identity, DID) hivatkozunk rájuk; egyébként általános értelemben vett (kriptográfiailag) verifikálható identitásként (verifiable identity, VID). Az explicit, tanúsítványoktól és jogosítványoktól függetlenített identitáskezelés lehetővé teszi az identitások felhasználó általi kezelésének számos forgatókönyvét, például számos identitás létrehozása, vagy az identitásokhoz kötött authentikációs követelmények dinamikus kezelése (egy alapvető példa a nyilvános kulcs frissítése).

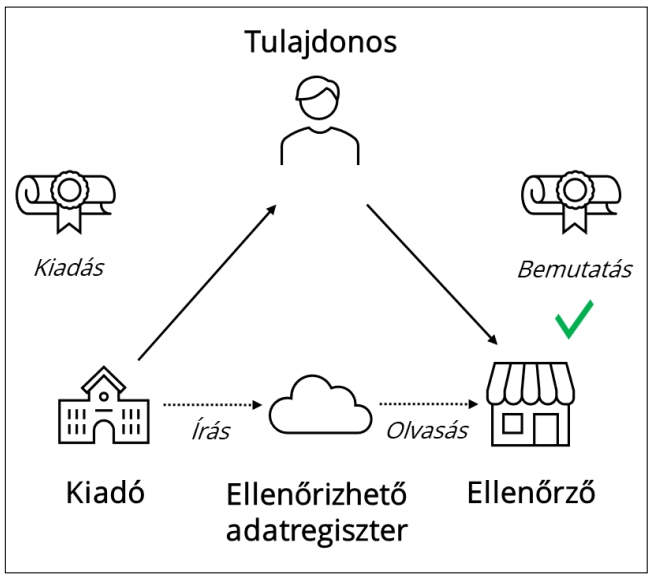
2.5. Ellenőrizhető tanúsítványok

A séma másik felét az úgynevezett ellenőrizhető tanúsítványok (verifiable credential, VC) adják. Megjegyzendő, hogy bár az angol terminológiában elválik a „credential” és a „certificate” fogalma, magyar fordításként mégis az „ellenőrizhető tanúsítvány” tűnik a legalkalmasabbnak, annak ellenére, hogy a tanúsítványt klasszikusan „certificate” értelemben használjuk.

Az ellenőrizhető tanúsítványok olyan digitális dokumentumok, melyeket egy kibocsájtó egy DID-re ad ki, a saját DID-jában meghatározott módon hitelesítve (digitálisan aláírva) ezeket. Ezek módosíthatóak és visszavonhatóak anélkül, hogy a visszavonás magát a DID-et érintené. Érett megoldások léteznek arra, hogy a tanúsítvány-ellenőrző felek egy tanúsítvány vissza nem vont voltát privacy-védő módon, a kibocsátók által nyilvánosan (például egy blokklánc felett) publikált és karbantartott, úgynevezett kriptográfiai akkumulátorokon keresztül végezzék. Maguk a tanúsítványok azonban nem kell, hogy ellenőrizhető adatregiszterben publikáltak és követettek legyenek; azokat tulajdonosuk tárolhatja kizárólag a tárcájában is.

A képet a blokklánc-technológiákban alkalmazásuk hatására széles körben ismertté vált tudásmentes bizonyítások (zero-knowledge proof, ZKP) [5] teszik teljessé:

megfelelően létrehozott VC-khez létrehozhatóak olyan ellenőrizhető matematikai bizonyítások, melyek csak a VC-be foglalt információk egy részét fedik. A szokásos iskolapélda a digitális személyi, mint ellenőrizhető tanúsítvány: míg a tanúsítványban számos érzékeny információ szerepel (pl. név, születési név, pontos születési idő és hely, anya leánykori neve), alkohol és dohánytermék vásárlásánál az ellenőrző fél számára ezek nagy része nem releváns – pusztán az, hogy a felmutatott tanúsítványt a megfelelő állami szerv adta-e ki, az érvényes-e jelenleg és hogy a tulajdonos 18 évnél idősebb-e. Ez utóbbi tulajdonság bizonyítható matematikailag ZKP-val úgy, hogy nemhogy a többi, tanúsítványba foglalt jellemző, de még a pontos születési idő sem kerül átadásra.



4. ábra Az SSI bizalmi háromszög

2.6. A bizalmi háromszög

Ezen elemekből áll össze a *4. ábrán* látható SSI „bizalmi háromszög” (trust triangle). A tanúsítványokat kiadó felek (Issuer) a tanúsítvány-tulajdonos (Holder) számára ellenőrizhető tanúsítványokat ad ki, az ellenőrzéshez szükséges adatokat – főként a saját identitását és a visszavont tanúsítványok kriptográfiai akkumulátorát – egy ellenőrizhető adatregiszterben kezelve; a tanúsítvány-ellenőrző fél a megfelelőségéről megbizonyosodhat a kiadóval való kommunikáció nélkül, pusztán az ellenőrizhető adatregiszterre támaszkodva.

3. Szabványtámogatás

Komoly technológiai-kísérleti előzmények és hosszú előkészítési folyamat után a World Wide Web Consortium (W3C) 2022 nyarán adta ki DID-ajánlásának 1.0 verzióját [6]; az erre épülő ellenőrizhető tanúsítvány adatmodell-ajánlás (Verifiable Credentials Data Model) már az 1.1 változatnál tart [7]. E két szabvány W3C-ajánlásként megjelenése alapvető fontosságú, annál is inkább, mert mögöttük egy sor, részben már ma is ipari érettségű implementáció áll.

A DID-szabvány kettéválasztja a DID „címzését” és tartalmát. Szigorúan véve egy DID egy *did:<metódus>:<metódus-specifikus azonosító>* szerkezetű karaktersorozat, amely egy úgynevezett DID-dokumentumra (DID Document) oldható fel *(5. ábra)*; a feloldás módját a metódus rész vezérli. A W3C-metódusok egy kanonikus regiszterét [8] is karban tartja; ezek között megtalálhatóak

– teljesen decentralizált megközelítések, mint az Ethereum nyilvános blokklánc feletti Ethereum Name Service-en (ENS) keresztül való DID-dokumentumfeloldás és -kezelés;
– szervezetek diverz, de jogosultságkezelt közössége által üzemeltetett blokkláncok feletti névfeloldás, melynek hozzáférése azonban nyílt: ilyen az EU tagállamai által üzemeltetett European Blockchain Services Infrastructure (EBSI); és
– klasszikus értelemben centralizált, illetve szervezetek közössége által üzemeltetett és csak számukra hozzáférhető blokkláncok.

Blokklánc alapon vagy sem, a DID-dokumentumokat kezelő ellenőrizhető adattár célja, hogy egy olyan megbízható platformot adjon, ahol a felhasználók biztosak lehetnek identitásaiknak az SSI-elveknek megfelelő kezelésében, és amit a DID-ekre épülő VC-ket ellenőrző felek is elégségesen megbízhatónak tartanak.

A VC-k adattartalmát a szabvány nem határozza meg, lehetséges szemantikájuk köre igen széles, az elektronikus személyitől a diplomákon és különböző felhatalmazásokon keresztül a kereskedelmi pontgyűjtőprogramok támogatásáig. Így az ellenőrizhető adattár egy másik fontos funkciója, hogy a VC-sémákat kezelje, és sokszor itt történik az ellenőrizhető tanúsítványok kiadásához kapcsolódó meghatalmazási lánc kezelése is (például egy központi oktatási hivatal által diplomák kiadására feljogosított szervezetek identitásainak kezelése).

A DID- és VC-szabványpár alapvetően adatmodell-jellegű; tényleges alkalmazásukhoz a következő protokollhierarchia szükséges:

- Az egyfajta „közszolgáltatásként” üzemeltetett ellenőrizhető adatregiszterek kezelési és elérési protokollja.
- A kommunikáló felek (illetve adattárcáik) közötti közvetlen kapcsolatfelépítés és közvetlen DID-csere protokollja.
- Adatcsere, kiadási és ellenőrzési protokollok az ellenőrizhető tanúsítványok szintjén (pl. kihívás-válasz azonosításra).
- Alkalmazási szintű protokollok és bizalmi ökoszisztémák (pl. oltási tanúsítványok és elfogadásuk szabályai).

Ezen protokollrétegeknek a szabványosítási törekvései részben folyamatosan zajlanak, részben pedig már ma is több lehetőség áll rendelkezésre megvalósításukra. Kiemelendő, hogy a műszaki interoperábilitás mellett mind a négy rétegben többszereplős irányítási problémák (az angol governance szó értelmében) is megoldandóak:

- Az ellenőrizhető adatregisztereknek megbízhatónak és pártatlannak kell lenniük: tartalmukat vagy egy

többszereplős konszenzusnak, vagy (állami) szabályozásnak kell szavatolnia.
- Meg kell teremteni az adattárcák és a végfelhasználók kommunikációját végző ágensek szabványosítási és adatvédelmi megfelelőségének, valamint megfelelőség-ellenőrzésének kereteit.
- Az ellenőrizhető tanúsítványok használatának szintjén a tanúsítványokkal kapcsolatos bizalom megteremtése nem műszaki kérdés; például a VC-ként kiadott diplomák hitelességét javallott egy „államilag regisztrált kibocsátó” mechanizmussal támogatni.
- Végül az ökoszisztémák szintjén a széles körű bizalom megteremtéséhez is szükséges a governance; a műszakilag természetesen adódó bizalmi integrációs lehetőségek (például oltási igazolványok sokszereplős elfogadása, vagy a kölcsönös diplomaelfogadás az EU országaiban) gyakorlati bizalmi aspektusai közel sem maguktól értetődőek.

A technológia és a governance rétegeit, valamint ezek még előttünk álló kihívásait független szereplőként elsődlegesen a Linux-alapítvány által létrehozott „Trust over IP” (ToIP) alapítvány vizsgálja [9]; a ToIP-alapítvány munkája részeként egy referencia-architektúrát is definiált.

4. Platformok és hálózatok

Az SSI-elvek és kialakuló szabványtámogatás első ipari minőségű és máig meghatározó platformját a Sovrin-alapítvány [10] hozta létre. A Sovrin-hálózat decentralizált, de üzemeltetésében nem szabad csatlakozású; üzleti modelljének alapgondolata az, hogy az adatregiszter írási operációiért kell fizetni. Bár önmagában a hálózat létrejötte is fontos SSI-mérföldkő volt (a „MainNet” 2017 óta üzemel), de talán még fontosabb, hogy az alapítvány a kódbázist a Hyperledger alapítvány égisze alatt nyílt forráskódúvá tette a Hyperledger Indy projektben (egyes komponensek később kiszervezésre kerültek a Hyperledger Aries projektbe).

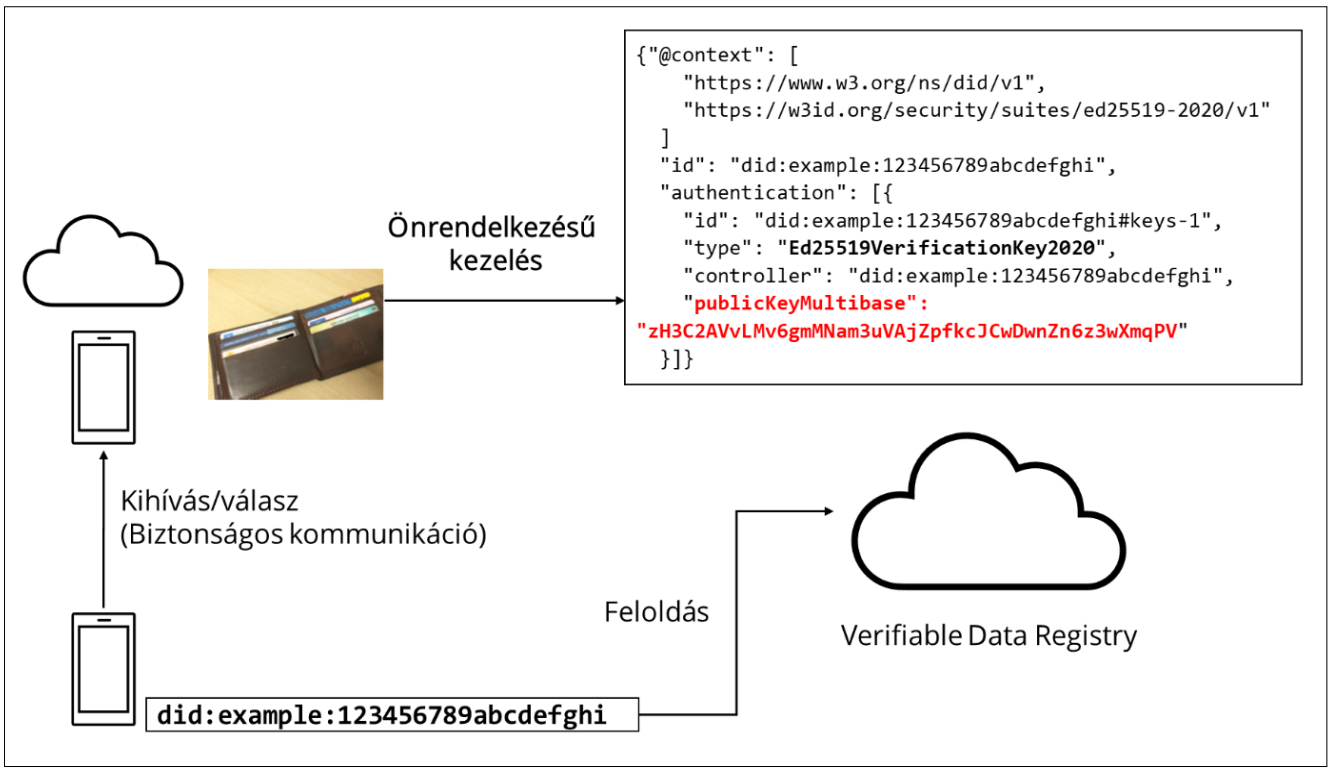
Az önrendelkezésű identitáskezelés és a felette megvalósítható ellenőrizhető tanúsítvány-interoperabilitás mind a digitális, mind az online identitáskezelés területén olyan transzformációs potenciállal rendelkezik, mely természetessé teszi azt, hogy bevezetésüket állami szereplők szorgalmazzák. Ma már több állami jellegű vagy erősen állami támogatású, illetve államközi, SSI-jellegű identitásszolgáltató hálózat üzemel, vagy áll kialakítás alatt. Ezek közül a talán legmeghatározóbbak az EBSI, az Alastria, a LACChain és az IDunion.

4.1. European Blockchain Services Infrastructure

Az EBSI-projektet [11] 2018-ban indította az Európai Bizottság és a European Blockchain Partnership (EBP), a tagállamok mellett Norvégia és Liechtenstein részvételével. A projekt egy olyan, a tagállamok kijelölt szervezetei által közösen üzemeltetett blokkláncplatformot épít ki, mely határokon átívelő, (tág értelemben vett) bizalmi szolgáltatásokat kínál.

Elsődleges célja jelenleg egy SSI-jellegű identitáskezelési réteg (European Self Sovereign Identity Framework, eSSIF) segítségével a közszolgáltatások támogatása, mint például a diplomák és egyéb felsőoktatási tanúsítványok határokon átnyúló ellenőrzése; távlatilag a rendszert az európai üzleti szféra számára is elérhetővé

5. ábra W3C DID és feloldása DI-dokumentumra



tervezik tenni (például adathitelesítésre, dokumentumkezelésre és eszközkövetésre). A kísérleti hálózat és használati eseteinek kidolgozása után az EBSI éles hálózatának kialakítása jelenleg is zajlik. Hazánk jelenleg három EBSI-csomópontjának egyikét a Budapesti Műszaki és Gazdaságtudományi Egyetem üzemelteti, a szerző szakmai vezetésével.

Az Alastria és a LACChain az EBSI-hoz nagyban hasonló kezdeményezések, előbbi az Ibériai-félszigeten, utóbbi Latin-Amerikában.

4.2. IDunion

Az IDunion [12] egy elsődlegesen német szövetségi támogatásból létrejött, de szervezetileg 2022 nyara óta európai szövetkezetként (Societas Cooperativa Europaea, SCE) üzemelő szervezet és hálózat. Sajátossága, hogy a természetes személyek mellett nagy hangsúlyt fektet a szervezetek és a „dolgok" (things) identitáskezelésének támogatására is – utóbbit deklarált módon az ipari IoT és az Ipar 4.0 egy fontos elemének tekintve.

A hálózat nem csak a szervezetek (ideértve a cégeket is) és az állampolgárok közötti megbízható azonosítást támogatja, de a szervezetek közötti biztonságos adatmegosztást is. A hálózat éles szolgáltatása várhatóan 2023 második felében indul.

4.3. KILT

Az elvi kiindulópontnak tekinthető, korlátozott, ám decentralizált és nem állami üzemeltetésű Sovrin-hálózathoz képest nem csak a „jobban szabályozott", illetve „zártabb", de a „teljesen decentralizált" irányban is számos komoly fejlesztés folyik. Ezek közül mindenképp kiemelésre érdemes a KILT-protokoll és -blokklánc, mely irányításában is teljesen decentralizált, mivel az a blokklánc kriptotoken-gazdaságához kötött. A KILT-blokkláncon kriptoeszközben való fizetéssel lehet DID- és VC regiszter-szolgáltatásokat igénybe venni és kifejezetten támogatja (digitális) eszközökhöz DID-k létrehozását és ezen DID-k más DID-khoz kötését, például tulajdonviszonyok követése céljából.

A KILT-blokklánc a Polkadot „blokkláncok blokkláncá" ökoszisztéma része, így távlatilag annak is egy modelljét adja, hogy az SSI hogyan integrálható egy elosztott főkönyvi ökoszisztémába és annak okosszerződéseibe.

5. SSI és Európa

Az EBSI-hálózat, mint kezdeményezés illeszkedik az Európai Bizottság biztonságos és megbízható európai digitálisidentitás-kezeléssel kapcsolatos törekvéseinek sorába.

Ennek hivatalos keretét a 910/2014/EU eIDAS (a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról) [13] rendelet felülvizsgálata és kiegészítése adja (az „eIDAS 2.0"), amelyhez kapcsolódóan megindult az európai digitális identitástárcák (European Digital Identity Wallet) referencia-architektúráinak [14] és kezdeti implementációinak kialakítása. Az identitástárcák várhatóan előírt képességként kell majd, hogy támogassák a W3C ellenőrizhető tanúsítványok kezelését (az ISO/IEC 18013-5 alapú digitális azonosítók mellett).

Így bár ma még nyílt kérdés, hogy specifikusan az EBSI, mint megoldás szerepe pontosan mi lesz az európai identitáskezelésben, de a nemzeti identitástárcák várhatóan képesek lesznek az EBSI-hálózat használatára is. Továbbá megjegyzendő, hogy az EBSI már ma is rendelkezik saját tárca-megvalósításokkal és tárca-megfelelőségi követelményrendszerrel, és eIDAS-kompatibilis azonosítást tesz lehetővé.

6. Ipari használati esetek

A decentralizált azonosítóknak és ellenőrizhető tanúsítványoknak számtalan magától értetődő alkalmazása adódik az állampolgárok, az állam és a szervezetek különböző azonosítási, tanúsítvány-, és jogosítvány-ellenőrzési viszonylataiban. A meglévő viszonylatokon túl már számos innovatív kezdeményezés is egyre inkább természetesen integrálja az SSI-megoldásokat, a blokklánc alapú élelmiszer-eredetkövetéstől a közeljövő digitális jegybankpénzekig (Central Bank Digital Currencies, CBDC).

Az ipar és a telekommunikáció számára is új lehetőségek nyílnak meg, különösen, ha az okos eszközök is önrendelkezésű identitásokat kapnak. A jelenleg elérhető (nyílt) végponti szoftver-megvalósítások körülbelül a közismert Raspberry Pi eszközök számítási teljesítményét igénylik; néhány folyamatban lévő fejlesztés eredményeként azonban már a közeljövőben várható, hogy az általános célú önrendelkezésű identitások natívan kezelhetővé váljanak jóval gyengébb SoC-megoldásokban is. Ipari alkalmazásként már ma is ismert az SSI bevezethetősége és előnyei

- a fizikai eszközök cégeken átnyúló, kollaboratív állapotmonitorozásban;
- követésükben, karbantartásukban és életciklus-kezelésükben, valamint
- a csalások elkerülésében.

7. Összefoglalás

Az identitásokat és jellemzőik bizonyítását szétcsatoló, önrendelkezésű identitástechnológiák széles körű bevezetésük és elterjedésük küszöbén állnak; cikkünk egy bevezető jellegű áttekintést adott a terület alapmegoldásairól, szabványairól és fejlődéséről.

Az önrendelkezésű identitások alkalmazásai ki fognak terjedni a digitális és online identitáskezelés klaszszikus forgatókönyveire, de egyúttal jóval túl is mutatnak azokon; várható, hogy az SSI-nek kulcsszerepe lesz az Ipar 4.0 és az ipari IoT szervezeti együttműködéseinek és dinamikusan kezelt infrastruktúráinak biztonságossá és megbízhatóvá tételében is.

Hivatkozások

[1] A. Christopher, “The Path to Self-Sovereign Identity”, *http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html*

[2] D. Vujičić, D. Jagodić and S. Randić, “Blockchain technology, bitcoin and Ethereum: A brief overview,” 17th International Symposium INFOTEH-JAHORINA, East Sarajevo, Bosnia and Herzegovina, 2018, pp.1–6., doi: 10.1109/INFOTEH.2018.8345547

[3] M. Rauchs et al., “Distributed Ledger Technology Systems: A Conceptual Framework,” 2018, SSRN-en: *https://ssrn.com/abstract=3230013,* doi: 10.2139/ssrn.3230013

[4] E. Androulaki et al., “Hyperledger fabric: a distributed operating system for permissioned blockchains,” In Proceedings of the Thirteenth EuroSys Conference (EuroSys ‘18), ACM, 2018, Article 30, pp.1–15. doi: 10.1145/3190508.3190538

[5] ZKProof Community, “ZKProof Community Reference,” *https://docs.zkproof.org/reference.pdf*

[6] World Wide Web Consortium, “Decentralized Identifiers (DIDs) v1.0”, *https://www.w3.org/TR/did-core/*

[7] World Wide Web Consortium, “Verifiable Credentials Data Model v1.1”, *https://www.w3.org/TR/vc-data-model/*

[8] World Wide Web Consortium, “DID Specification Registries – DID Methods”, *https://w3c.github.io/did-spec-registries/#did-methods*

[9] Trust over IP alapítvány, “The Trust over IP model”, *https://trustoverip.org/wp-content/toip-model/*

[10] A Sovrin-alapítvány honlapja, *https://sovrin.org/*

[11] Európai Bizottság, a European Blockchain Services Infrastructure honlapja, *https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Home*

[12] Az IDunion európai szövetkezet honlapja, *https://idunion.org/*

[13] Az Európai Parlament és Tanács 910/2014/EU rendelete (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, *https://eur-lex.europa.eu/legal-content/HU/ALL/?uri=CELEX:32014R0910*

[14] Európai Bizottság, “The European Digital Identity Wallet Architecture and Reference Framework,” *https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-wallet-architecture-and-reference-framework*

[15] F. Marquart, S. Bin. Shams, “Bringing Trustworthiness in Industrial Device Lifecycle using Verifiable Credentials,” *https://hgf22.sched.com/event/14H61*

A szerzőről

KOCSIS IMRE adjunktus, vezető blokklánc-kutató a Budapesti Műszaki és Gazdaságtudományi Egyetem (BME) Méréstechnika és Információs Rendszerek Tanszékén. Műszaki informatikus diplomáját, majd PhD-fokozatát is a BME-n nyerte el. Specializációja a blokklánc-technológiák ipari és szervezetközi alkalmazásai, valamint a blokklánc-alapú megoldások szolgáltatásbiztonságra és teljesítményre tervezése és validációja. A Hyperledger alapítvány felé a BME fő koordinátora, valamint az egyetem EBSI-csomópontjához kapcsolódó tevékenységek vezetője.