Uno schema simmetrico per lo scambio di credenziali di identità basato sul paradigma della fiducia, parte 2

Implementazione del servizio di fiducia dell'identità

Identificare un soggetto reale in rete, partendo dal suo nome digitale (username), è un compito reso possibile dal sistema di autenticazione. Prima riconosce la validità dell'identità digitale e poi associa le informazioni personali che ha ricevuto nella registrazione del soggetto. In molte altre situazioni, è sufficiente la sola validità dell'identità digitale per attivare un servizio. Ad esempio, un abbonamento gratuito ad una newsletter via email. Purtroppo, nella registrazione spesso sono richiesti dei dati personali aggiuntivi e non necessari al fine del riconoscimento del soggetto fisico. Chi richiede i dati presuppone di averne sempre il diritto, giustificato dalla mancanza di metodi di identificazione alternativi, e chi li consegna non ha il tempo e la capacità di verificare l'efficacia delle eventuali garanzie offerte, comprese quelle legali. Ulteriore problema, non c'è garanzia dell'efficacia del controllo sui dati registrati, a volte basta una fotocopia della carta d'identità per attivare una nuova identità digitale. E se la fotocopia era stata rubata?

Questo approccio deve essere riequilibrato con un riconoscimento simmetrico tra le due parti che si devono identificare. Il metodo proposto assegna pari diritti ad entrambe le parti e ne richiede una reciproca identificazione basata sulla garanzia dell'effettiva identità stabilita da due fiduciari, uno per ciascuna parte, per questo è detto "double trustee".

LUIGI SBRIZ | CISM, CRISC, CDPSE, ISO/IEC 27001:2013 LA, ITIL V4, UNI 11697:2017 DPO

È stato responsabile del monitoraggio dei rischi presso un'azienda multinazionale del settore automotive per oltre sette anni. In precedenza, è stato responsabile della gestione dei servizi e delle risorse ICT nell'area Asia-Pacific (Cina, Giappone e Malesia) e, prima ancora, è stato responsabile della sicurezza delle informazioni a livello mondo per più di sette anni. Per quanto attiene al monitoraggio interno del rischio, ha sviluppato una metodologia originale integrando tra loro, analisi del rischio operativo, valutazione del livello di maturità dei controlli e risk-based Internal Audit. I processi aziendali sono paragonati a servizi cooperanti basati sui principi guida del framework ITIL 4 e del Manifesto Agile. Inoltre, ha progettato uno strumento di cyber monitoring e un sistema integrato per monitoraggio del rischio, modello di maturità e audit interno. Sbriz è stato anche consulente per sistemi di business intelligence per parecchi anni. Può essere contattato su LinkedIn a *https://it.linkedin.com/in/luigisbriz* oppure tramite *http://sbriz.tel.*

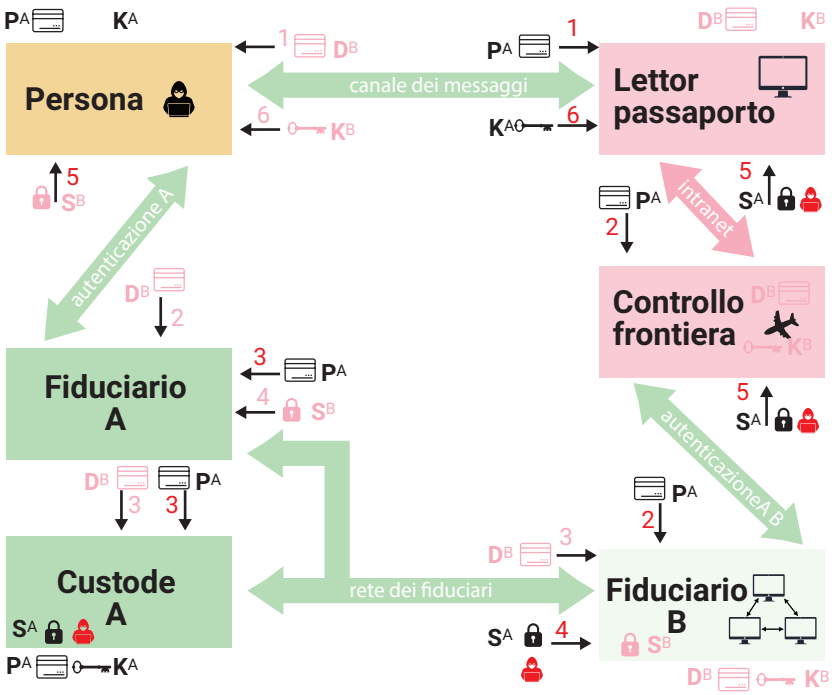
Attuazione di un mezzo per gestire l'identità digitale basata sul concetto di identità fiducia, come discusso nella parte 1 di questa serie, "Modello astratto di fiducia dell'identità"[1], è meglio descritto utilizzando una situazione complessa dalla vita reale come esempio. Il controllo del passaporto è un esempio eccellente perché comprende diverse questioni impegnative, incluso l'organizzazione della rete dei fiduciari su due livelli, gestendo più punti di autenticazione per entità complesse e considerando le imprese internazionali che gestiscono la rete dei fiduciari.

Esempio del controllo passaporti

L'aeroporto rappresenta una tipica entità complessa, nel senso che eroga un servizio di identificazione per tramite di innumerevoli stazioni di riconoscimento, coordinate da un centro di comando operazioni. Ogni stazione deve avere la capacità di assolvere completamente a tutte le formalità di identificazione nel rispetto di rigide norme. Tutti i passaporti sono dotati di microchip che conserva le informazioni personali ed è usato per automatizzare il processo (ossia, rendere alcune informazioni disponibili ai lettori automatici per il controllo). Altre informazioni possono essere richieste, dalle autorità aeroportuali a quelle del paese di emissione del passaporto.

FIGURA 1

Schema di identificazione simmetrica con identità fisica



Il processo di verifica passaporti rappresentato in **figura 1** può essere usato come esempio per comprendere lo schema simmetrico di identificazione con l'identità fisica. Inoltre, il principio del need-to-know (ossia, è permesso accedere ad una risorsa avendo il giusto livello di sicurezza e la necessità operativa, ma non è permesso accedere a risorse prive di questi due requisiti), tipico della protezione dati personali, sarà continuamente applicato, sia per minimizzare il rischio di utilizzi impropri dei dati che per permettere un processo più efficiente (nessuna ridondanza).

L'identità fisica è custodita da un trustee detto custode. Il custode ha l'autorità legale per il riconosciuto fisico del proprietario dell'identità digitale ed proteggere i relativi dati personali. Pertanto, nella rete dei trustee ci sono due tipi di nodi: il custode dell'identità fisica, che gestisce i dati personali, ed il trustee dell'identità digitale, che gestisce l'autenticazione dello username che circola in rete. Ogni entità, può richiedere più di una identità digitale, sia allo stesso trustee che a diversi.

Nell'aeroporto, l'autorità nazionale di controllo delle frontiere, è responsabile per l'esecuzione del controllo dei passaporti per tramite di diverse postazioni fisiche di lettura passaporti, presidiate da personale o self-service automatici. Per una gestione più efficace, questa autorità richiede di essere identificata come un'unica entità dal trustee. In tal modo, viene emessa una sola carta d'identità digitale all'autorità nell'aeroporto ed è gestita da un sistema centrale che farà da hub per tutti i lettori dislocati nell'aeroporto. Tutte le postazioni di controllo passaporti dislocate nell'aeroporto, condivideranno le stesse credenziali presenti nel sistema centrale, salvo una necessaria distinzione nell'indirizzo fisico in rete e nell'identificativo del dispositivo. Nel badge ci saranno dei selettori per indicare se il mittente è una entità od un dispositivo (in conseguenza, dei campi opzionali predefiniti avranno le coordinate del sistema hub in quanto solo quest'ultimo si potrà interfacciare con il trustee).

Si suppone che la persona sia dotata del proprio smartphone per l'accesso al fiduciario. In caso contrario, verrà usato il microchip del passaporto ma il livello di sicurezza sarà inferiore perché il meccanismo non sarà simmetrico. Il processo di identificazione tra la persona (badge P^A) ed il lettore di passaporti (badge D^B) può avviarsi con la lettura di un QR code[2]

visibile presso il chiosco del controllo passaporti, o con analoghe tecnologie contactless. Il QR code sarà un semplice URL associato al lettore passaporti per visualizzare il form con l'informativa sul trattamento dati e la richiesta del consenso all'invio dei dati personali (questo passo attiva lo scambio dei badge). Le sei fasi per l'identificazione sono:

1. La persona usa lo smartphone per scambiare i badge digitali, (P^A e D^B), con il lettore di passaporti. La persona aggiorna il badge rifacendo l'autenticazione sul proprio trustee. Tra i dati che dovrà comunicare al proprio trustee, ci sarà anche un flag per richiedere l'invio della propria identità reale al lettore di passaporti. Il lettore di passaporti ha il badge dell'aeroporto (identità digitale) che è stato fornito dal sistema hub dell'autority, il quale lo ha ricevuto dal Trustee B. Una policy a tempo decide quando aggiornare nuovamente i badge di tutti i lettori attivi.
2. Lo smartphone della persona ed il lettore di passaporti inviano al proprio fiduciario il badge ricevuto dalla controparte. Il badge D^B va al Trustee A (includendo in automatico la lista delle categorie dei dati personali da comunicare) mentre il badge P^A va al Trustee B tramite inoltro fatto dal sistema hub dell'autorità di frontiera.
3. I due fiduciari si scambiano i badge digitali, P^A e D^B, ricevuti dalla propria entità. Poi, il Trustee A, appena riceve il badge P^A a conferma che il badge D^B è reale, inoltra i due badge al Custode A. Il badge P^A serve per il test di integrità, il badge D^B per conoscere i dati del Trustee B e del suo richiedente. Il custode potrebbe anche rifiutarsi di inviare le informazioni personali se ritiene che il destinatario non offra tutele sufficienti.
4. Il fiduciario B prepara il sigillo S^B e lo inoltra al fiduciario A. Il custode A prepara il sigillo S^A e lo inoltra al fiduciario B. Tutti i sigilli sono di una dimensioni standard, anche se potrebbero non includere tutte le informazioni personali richieste. Ciò mantiene le informazioni più sicure perché non vi è alcuna differenza apparente tra sigilli di identità personale e digitale. È più difficile per un malintenzionato osservatore del traffico di rete identificare i dati personali quando vengono utilizzati sigilli di dimensioni standard. I dati mancanti saranno però accessibili al destinatario tramite un link ed una chiave crittografica (specifica del lettore di passaporti), opportunamente inseriti nel sigillo.
5. I sigilli sono inoltrati dai fiduciari alle entità senza compiere alcuna operazione ulteriore. Nel caso del sigillo S^A, l'entità ricevente sarà il sistema hub dell'autorità di frontiera, che lo inoltrerà al corretto lettore di passaporti.
6. Appena arrivano i sigilli, lo smartphone della persona ed il lettore di passaporti si scambiano le chiavi digitali, K^A e K^B, per permettere l'apertura. Il lettore di passaporti provvederà a recuperare eventuali dati personali aggiuntivi nel caso in cui non vi sia spazio sufficiente nel sigillo per il messaggio completo.

Sembra un meccanismo complesso ma in realtà ci sono solo poche operazioni da svolgere e computazionalmente semplici. Può sembrare più semplice leggere il microchip nel passaporto ma le informazioni che contiene non sono verificabili in tempi brevi e non gestisce con efficacia eventuali aggiornamenti. Il badge dei dati personali contiene gli indicatori di selezione delle categorie dei dati personali da inviare. Le categorie, intese come blocchi di dati, devono essere codificate secondo uno standard aperto per produrre dei messaggi facilmente interpretabili, ad esempio tramite il protocollo Multipurpose Internet Mail Extensions (MIME)[3]. Questo è un metodo semplice usato per incapsulare contenuti differenti ed associarli ad un indirizzo del tipo, nome dell'interessato, un simbolo separatore ed il nome a dominio del identity provider. La scelta di quali categorie inviare è fatta nel form di consenso sull'invio. Esempio di categorie potrebbero essere, dati anagrafici, dati sanitari (vaccinazioni, gruppo sanguineo, allergie…), passaporto (numero, fototessera, contatti per emergenze, visti attivi…) e così via. Il default è inviare solo il nome reale, ogni blocco di dati aggiuntivi richiederà il consenso.

Considerazioni implementative

Si può ipotizzare che possano esistere più identità digitali per ciascun soggetto fisico e quindi, nel dispositivo usato per il processo di identificazione, ci sarà una cassaforte per contenerle. La cassaforte delle identità digitali è aggiornata possibilmente in fase di autenticazione con il trustee, con i dati correnti di identificazione in rete del dispositivo ed i dati di riconoscimento dell'identità richiesti dal processo di autenticazione. Il canale di comunicazione è sempre crittografato ed anche se non è una misura di sicurezza assoluta, si aggiunge a tutte le altre per contribuire al rafforzamento della protezione

da tentativi di ascolto non autorizzato del traffico dati. L'obiettivo non è di assicurare l'impossibilità di accesso ai dati ma di ritardare l'utilizzabilità delle informazioni contenute finché l'identificazione è accettata o rifiutata. Ogni nuova autenticazione rende nulle le informazioni precedenti riaggiornando le credenziali di riconoscimento.

L'identità digitale è rappresentata da una username creata come l'indirizzo di una casella di posta elettronica. Sarà nel formato avatar_name@trustee.home con "avatar_name" il nome scelto per identificarsi nel cyberspazio, "trustee" il nome del dominio associato al fiduciario ed "home" il codice del Paese tratto dallo standard ISO 3166-1 alpha-2[4], sede legale del fiduciario. L'identità digitale serve a tutelare i dati personali dell'identità reale ma il fiduciario non potrà mai essere meramente virtuale. Per assicurare completa fiducia, deve essere garantita piena tutela ai dati delle entità che si rifanno ad un certo fiduciario e quindi devono essere dei soggetti pubblici con vincoli legali.

Il processo di riconoscimento si svolge nella pratica a partire dal form di identificazione, emesso da uno dei due soggetti, dove al posto del campo password c'è un selettore dei metodi possibili di identificazione. Esempi di scelte possono essere la normale password, oppure un'identità digitale di fiducia oppure una strong authentication o altro. Tra l'altro, in questo modo, non abbiamo necessità di diversificare i nomi delle identità. Possiamo usare la stessa identità con più meccanismi di identificazione, configurati a priori e scelti sulla base del livello di rischio accettato. Questi i passi generali per identificarsi con l'identità digitale.

1. Inserire lo username (nome dell'identità digitale).
2. Selezionare il tipo di identificazione (con o senza invio di dati personali).
3. Sulla scelta fatta, aggiornare le credenziali con il proprio fiduciario oppure usare quelle in cassaforte.
4. Automaticamente il dispositivo invia il badge, attende ed invia il badge dell'altra entità, attende il sigillo, lo apre ed invia la chiave all'altra entità.
5. Se il sigillo si apre, allora l'identità è confermata altrimenti interrompe il processo.

Il modello funzionale dell'identity provider può basarsi su framework esistenti, ad esempio il Security Assertion Markup Language (SAML[5]) che permette la realizzazione di un sistema sicuro di single sign-on (SSO) federato. Il meccanismo di comunicazione tra differenti identity provider deve essere aggiunto, per questo al nome dell'interessato si deve aggiungere il nome dell'identity provider prescelto.

Come affrontare le situazioni anomale

In qualunque nodo si può verificare una non-accettazione del messaggio circolante per disallineamento di informazioni o problemi di integrità. Il processo si interrompe nel primo nodo dove si verifica una qualunque situazione anomala e superato il tempo di vita del ciclo in ogni nodo, annulla la prosecuzione dell'identificazione senza rilasciare alcun messaggio. Il mancato invio di risposte negative a seguito di anomalia interrompe la diffusione di indicatori che le credenziali possano essere state usate da parte di soggetti malevoli. L'annullamento per qualsiasi ragione richiede la ripartenza del ciclo di verifica con l'emissione di nuove credenziali.

Per contrastare le attività di intercettazione, i messaggi del badge, del sigillo e della chiave devono avere una lunghezza fissa standard, indipendentemente dalla quantità dalle informazioni che contengono, ed essere crittografati. Il livello di robustezza della crittografia non è molto importante, meglio privilegiare la sua efficienza nel farlo.
La crittografia deve resistere solo per il tempo necessario a chiudere il ciclo di identificazione, l'eventuale riavvio avverrà con nuove credenziali.

Emissione di una nuova identità digitale

Il custode è un gestore legale dei dati personali, nominato da un autorità governativa del Paese ove ha residenza legale la persona che richiede il rilascio di una identità digitale. Questa attività prevede il riconoscimento della persona reale e di una suo primo dispositivo detto master. Il custode procede al riconoscimento della persona o tramite la presenza fisica dell'interessato, o in una sessione online, con esibizione dei documenti ufficiali di identità. Ulteriori dispositivi possono essere aggiunti per conferma tramite il primo dispositivo. Nel tempo il master può essere sostituito da uno degli altri dispositivi, tramite una semplice procedura online automatizzata. Periodicamente, anche i dati di riconoscimento personale, come la fototessera, vanno aggiornati secondo una pianificazione stabilita dall'autorità governativa o più frequente stabilita dal custode in caso di rischio o di incidenti.

La fase propedeutica a qualsiasi richiesta di identità digitale è la registrazione dei propri dati personali presso il custode che rilascerà un badge digitale P^A per potersi registrare in seguito presso qualsiasi trustee si voglia. Il badge digitale P^A è identificato da una username nel formato "hex_string@custodian.home" dove "hex_string" è una sequenza, a lunghezza fissa, di caratteri esadecimali definita in modo randomico dal custode. Non contiene alcun riferimento né alla persona né alla data di emissione e può essere rinominata con richiesta al custode. Si suggerisce un formato di tipo prefisso concatenato a un codice di controllo, quest'ultimo può essere costruito con semplicità da "prefisso MOD 13" (o altro modulo[6]) per intercettare un eventuale errore di inserimento.

Ricevuto il badge personale, che non contiene dati personali ma un identità digitale garantita dal custode, si può procedere alla richiesta di una o più identità digitali. La creazione di una nuova identità digitali si svolge in quattro fasi, come viene illustrato nella **figura 2**:

1. La persona A invia al fiduciario B il badge digitale P^A, rilasciato dal custode A e riceve il badge D^B. Il badge P^A contiene un flag che definisce questo scambio di messaggi come una registrazione presso un fiduciario. Lo username proposto conterrà il dominio del fiduciario.
2. La persona A ed il fiduciario B inviano rispettivamente i badge D^B e P^A al custode A. Il badge D^B conterrà un campo informazione con il nuovo username scelto dalla persona A.
3. Il custode A prepara il sigillo S^A con i dati di registrazione della persona fisica secondo quanto definito dallo standard.
4. La persona A ed il fiduciario B ricevono il sigillo ed alla ricezione, la persona A invia al fiduciario B la chiave K^A per aprire il sigillo.

Le identità digitali sono gestite dai fiduciari e quindi è ragionevole aspettarsi di sostenere un equo costo, tramite abbonamento annuo, come se stessimo acquisendo un nome di dominio su Internet. Il pagamento serve anche ad evitare eccessi, sia nel numero di identità possedute che nella frequenza di rinomina dell'identità. Una identità dismessa, deve rimanere archiviata per tracciabilità del proprietario per un periodo sufficientemente lungo da ritenere che non ci possano essere delle truffe per scambio di identità.

Delle blockchain gestite dai fiduciari garantiscono il log temporale delle registrazioni, delle cancellazioni e delle operazioni di identificazione utili in caso di un attività forense. I fiduciari possono essere le stesse società che gestiscono i nomi a dominio dei siti oppure i gestori di server di posta pubblici ma devono essere soggetti a specifica certificazione di sicurezza, a tutela delle entità che registrano la propria identità. Un'autorità internazionale di controllo dei fiduciari è pertanto indispensabile.

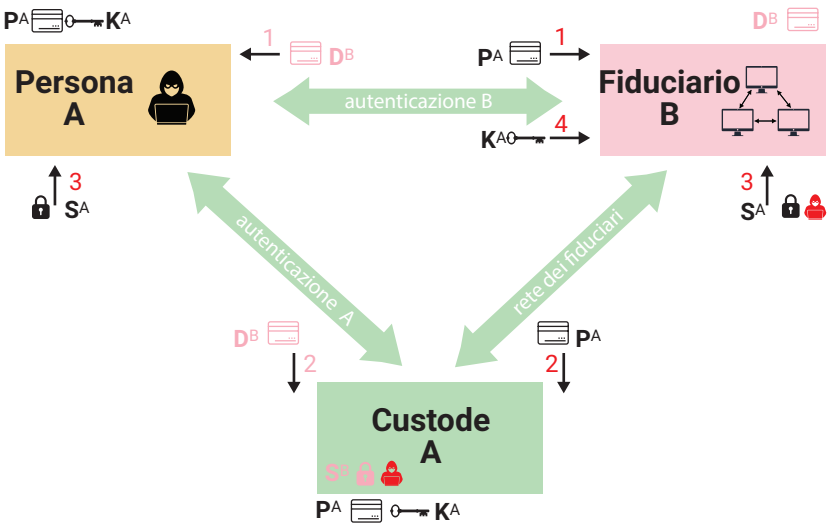
Conclusioni

La soluzione proposta, affronta il tema del riconoscimento reciproco di due entità, senza una preventiva registrazione di dati personali su ogni nuovo sistema di autenticazione, mantenendo così un lecito anonimato. Nello stesso tempo è necessario garantire alle autorità ogni azione idonea a contrastare le frodi conseguenti ai furti d'identità, in quanto, l'anonimato assoluto non si armonizza con l'esigenza di stipulare accordi. Si deve bilanciare la tutela del rispetto di rapporti contrattuali con la garanzia di un uso consapevole dei dati personali. Quindi, l'identità digitale non rappresenta il nome reale di un entità fisica ma un puntatore virtuale per eventualmente permettere alle autorità locali di risalire al fiduciario e da questo al custode. Solo le autorità del Paese di residenza del custode, o di una sua entità, avranno la facoltà di accedere a tutti i dati personali.

Per rendere effettivo questo meccanismo, è indispensabile assegnare ad una singola autority

FIGURA 2

Creazione di una nuova identità digitale



internazionale il potere di regolamentazione dell'operato dei trustee, dei formati dei messaggi, di gestione della rete dei trustee e di governo dei controlli sul rispetto delle norme. Questa autority contribuisce a preservare la qualità del servizio ma soprattutto il rispetto di un codice etico a tutela dei soggetti identificati. I fiduciari devono svolgere i loro compiti nella massima trasparenza per meritarsi la fiducia concordata. La loro prima responsabilità è di garantire l'autenticità dei messaggi e nessun ulteriore trattamento diverso dall'identificazione dell'entità può essere ammesso sui dati trattati, espressamente vietata la profilazione utente. Inoltre, su mandato dell'autority, un controllo sistematico delle attività del trustee da parte di enti esterni di certificazione è funzionale a conservare il clima complessivo di fiducia nelle operazioni svolte. In aggiunta, i custodi, dovrebbero essere vincolati a privacy audit periodici da parte delle autorità legalmente competenti sui dati trattati.

Infine, una considerazione sull'etica della limitazione di libertà. Il problema dell'eccessivo uso di dati personali è trasformato nella dimostrazione della titolarità ad utilizzare uno specifico username, in un determinato momento. Questo metodo favorisce un lecito anonimato, in quanto esclude all'entità controparte la necessità di conoscere i nostri dati personali, nel caso sono comunicati solo con il consenso, ed assegna ad un garante (di nostra fiducia) della nostra identità digitale, i criteri per risalire ai nostri dati reali, con il solo intento di prevenire ogni forma di abuso. Possiamo vedere in questo una perdita controllata del nostro anonimato.

La nostra identità reale non può essere usata a nostra insaputa ma nello stesso tempo non siamo del tutto anonimi, la legittima autorità può rintracciarci. In Internet, l'agire in libertà è sacro ma sempre bilanciato dalla responsabilità delle proprie azioni.

Riferimenti

1 Sbriz, L.; "A Symmetrical Framework for the Exchange of Identity Credentials Based on the Trust Paradigm, Part 1,: *ISACA® Journal*, vol. 2, 2022, *https://www.isaca.org/archives*

2 International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), ISO/IEC 18004:2015 *Information Technology—Automatic Identification and Data Capture Techniques—QR Code Bar Code Symbology Specification*, Switzerland, 2015, *https://www.iso.org/standard/62021.html*

3 Techopedia, "Multipurpose Internet Mail Extensions (MIME)," 1 February 2017, *https://www.techopedia.com/definition/1693/* multipurpose-internet-mail-extensions-mime

4 International Organization for Standardization (ISO), ISO 3166-1:2020 *Codes for the Representation of Names of Countries and Their Subdivisions—Part 1: Country Code*, Switzerland, 2020, *https://www.iso.org/standard/72482.html*

5 OASIS Open, OASIS Security Services (SAML) TC, *https://www.oasis-open.org/committees /tc_home.php?wg_abbrev=security*

6 Gauss, C.; A. A. Clarke; Disquisitiones Arithmeticae, English Edition, Yale University Press, USA and UK, 2009