PERSONAL IDENTITY

PIV: Verifica dell'Identità Personale

Autore: Aldo Pedico – Enterprise Security & Privacy
Contatto: pedicoaldo@gmail.com

STORIA

Nel 2004, al fine di eliminare le ampie variazioni nella qualità e nella sicurezza dei meccanismi di autenticazione utilizzati nelle agenzie federali, la Direttiva Presidenziale statunitense sulla Sicurezza Interna (HOMELAND SECURITY PRESIDENTIAL DIRECTIVE-12 - HSPD-12) *richiede l'implementazione delle* PIV CARD *e della loro infrastruttura di supporto.*

La direttiva richiedeva uno standard di identificazione comune per promuovere meccanismi d'autenticazione interoperabili a livelli di sicurezza graduati in base all'ambiente e alla sensibilità dei dati.

In risposta, il FEDERAL INFORMATION PROCESSING STANDARD (FIPS) 201 *del 2005 ha specificato un insieme comune di credenziali in un fattore di forma di* smart card, *noto come* PERSONAL IDENTITY VERIFICATION (PIV) CARD, *per l'accesso fisico e logico alle strutture governative e ai sistemi informativi federali.*

Al momento della prima pubblicazione di FIPS 201, l'accesso logico era orientato ai dispositivi informatici tradizionali (ad esempio computer desktop e laptop) in cui la PIV Card fornisce meccanismi di autenticazione comuni tramite lettori integrati in tutto il governo federale. Con l'emergere di una nuova generazione di dispositivi informatici e in particolare con i dispositivi mobili, l'uso delle carte PIV si è rivelato impegnativo.

I dispositivi mobili non dispongono dei lettori di smart card integrati presenti nei computer portatili e desktop e richiedono lettori di schede separati collegati ai dispositivi per fornire servizi di autenticazione dal dispositivo.

Per i reparti e agenzie statunitensi l'utilizzo di PIV Card e lettori di card separati è stata una soluzione pratica per l'autenticazione dai dispositivi mobili, sfruttando il NEAR FIELD COMMUNICATION (NFC) *per comunicare con la scheda PIV.*

INTRODUZIONE

*Nei capitoli seguenti si espone il processo per la ricerca delle credenziali (*PROOF OF CONCEPT*) ai fini della* VERIFICA DELL'IDENTITÀ PERSONALE *(*PERSONAL IDENTITY VERIFICATION – PIV*).*

Le PIV CARD basate su smart card non possono essere utilizzate prontamente con la maggior parte dei dispositivi mobili, come smartphone e tablet, mentre le credenziali PIV DERIVATE *(*DERIVED PIV CREDENTIAL - DPC*) possono essere utilizzate su questi dispositivi per fornire l'autenticazione a più fattori (*MULTI-FACTOR AUTHENTICATION*) agli utenti.*

Questo documento evidenzia i requisiti esistenti relativi ai DPC e propone un'architettura che supporti tali requisiti e quindi dimostri come tale architettura possa essere implementata e gestita.

INDICE DEGLI ARGOMENTI

1. BUSINESS OPPORTUNITIES FOR USING DPCS WITH MOBILE CLIENT DEVICES

CHALLENGES WITH USING PIV CARDS ON MOBILE DEVICES

Il principio del "privilegio minimo", cioè "concedere agli utenti solo gli accessi di cui hanno bisogno per svolgere le loro funzioni ufficiali", richiede sia processi di autenticazione sia di autorizzazione.

FIPS 201-2 consiglia di utilizzare smart card X.509 con i dati dell'utente insieme a password/numeri di identificazione personale (PIN) per fornire l'autenticazione a due fattori ai sistemi informativi.

Le organizzazioni che si affidano all'autenticazione a due fattori con smart card e password devono autenticare gli utenti dei dispositivi mobili in un modo sia più resistente, alle manomissioni rispetto a una password, sia facile da usare come una smart card.

Tuttavia, è difficile utilizzare le smart card sui dispositivi mobili a causa del loro fattore di forma.

Il collegamento o il TETHERING *di un lettore di smart card esterno separato a smartphone o tablet crea problemi di usabilità e portabilità che rendono la carta un token di autenticazione poco pratico.*

PROPOSED SOLUTION: DPCS

NIST SP 800-157 definisce l'uso di un DPC come una possibile soluzione per abilitare PIV a un dispositivo mobile, specificando l'uso di token crittografici su dispositivi mobili in cui possono essere utilizzati DPC e le loro chiavi private corrispondenti.

Questa soluzione sfrutta un'infrastruttura a chiave pubblica (PKI) con credenziali derivate da una carta PIV.

I DPC basati su X.509 sanno utilizzati per l'accesso logico alle risorse remote ospitate all'interno di un data center o nel cloud.

La corrispondente chiave privata derivata (DERIVED PRIVATE KEY) *sarà memorizzata in un modulo crittografico con un fattore di forma alternativo come hardware o software incorporato in un dispositivo mobile o un token rimovibile (ad es. una scheda* Secure Digital - SD, Universal Integrated Circuit Card - UICC, *la nuova generazione di schede* Subscriber Identity Module – SIM, *token* Universal Serial Bus - USB*).*

DPC REQUIREMENTS

Questa sezione riassume i requisiti durante le attività primarie del ciclo di vita per il DPC come descritto in NIST SP 800-157.

Per ottenere l'interoperabilità con l'infrastruttura PIV e le sue applicazioni, la soluzione utilizza la tecnologia PKI come base per il DPC.

GENERAL REQUIREMENTS

- *Emissione di un DPC per il quale la corrispondente chiave privata è memorizzata in un modulo crittografico che costituisce un fattore di forma alternativo alla PIV Card.*
- *Uso di token con fattori di forma alternativi alla PIV Card che possono essere inseriti in dispositivi mobili, come token micro SD, token USB, UICC o incorporati nel dispositivo mobile o informatico.*

- *I DPC basati su PKI specificati in questo documento sono rilasciati ai livelli di garanzia (*LEVEL OF ASSURANCE - LOA*) 3 e 4.*
- *I DPC si basano sul concetto generale di credenziale derivata (vedi NIST SP 800-63-2) che sfrutta la verifica dell'identità e i risultati del controllo delle credenziali correnti e valide*
- *Il richiedente per ricevere un DPC deve dimostrare il possesso di una PIV Card valida.*
- *Il certificato di autenticazione PIV derivato è un certificato a chiave pubblica X.509 emesso in conformità con i requisiti di NIST SP 800-157 e X.509 Certificate Policy.*
- *La firma digitale e le chiavi di gestione delle chiavi possono essere incluse sui dispositivi mobili.*

INITIAL ISSUANCE REQUIREMENTS

- *Un DPC deve essere rilasciato a seguito della verifica dell'identità del Richiedente utilizzando la chiave di autenticazione PIV sulla sua PIV Card esistente dimostrando il possesso e il controllo della relativa PIV Card tramite il meccanismo di autenticazione PKI-AUTH di cui alla Sezione 6.2.3.1 di FIPS 201- 2.*
- *Lo stato di revoca del certificato di autenticazione PIV del richiedente deve essere ricontrollato sette giorni di calendario dopo l'emissione del DPC.*
- *Un DPC può essere rilasciato a livello di assicurazione dell'identità tre o quattro (LOA-3 o LOA-4).*
- *Un DPC LOA-3 può essere rilasciato a distanza o di persona, mentre un DPC LOA-4 viene rilasciato di persona in conformità con NIST SP 800-63-2.*
- *Se la credenziale viene rilasciata a distanza, tutte le comunicazioni devono essere autenticate e protette da modifiche (ad esempio, utilizzando Transport Layer Security (TLS)) e la crittografia deve essere utilizzata per proteggere la riservatezza di qualsiasi dato privato o segreto.*
- *Se il processo di rilascio prevede due o più transazioni elettroniche per un DPC LOA-3, il richiedente deve identificarsi in ogni nuovo incontro presentando un segreto temporaneo che è stato rilasciato in una transazione precedente, come descritto nella Sezione 5.3.1 del NIST SP 800-63-2.*
- *Il richiedente deve identificarsi utilizzando un campione biometrico che può essere verificato rispetto alla carta PIV del richiedente al momento dell'iscrizione a un DPC LOA-4.*
- *Se ci sono due o più transazioni durante il processo di emissione, il richiedente deve identificarsi utilizzando un campione biometrico che può essere verificato sia rispetto alla Carta PIV sia rispetto a un biometrico registrato in una precedente autorizzazione al momento dell'emissione di un LOA-4 DPC.*
- *Se è stata emessa una credenziale LOA-4, l'emittente deve conservare per riferimento futuro il campione biometrico utilizzato per convalidare il richiedente.*
- *Il NIST SP 800-157 non preclude il rilascio di più DPC allo stesso Richiedente sulla base della stessa Carta PIV.*

MAINTENANCE REQUIREMENTS

- *Quando la chiave del certificato o la modifica viene eseguita in remoto per un DPC LOA-4, la comunicazione tra l'emittente e il modulo crittografico, in cui è archiviata la chiave privata di*

autenticazione derivata da PIV, deve avvenire solo su sessioni sicure reciprocamente autenticate tra moduli crittografici testati e convalidati.

- *Quando la chiave o la modifica del certificato viene eseguita in remoto per un DPC LOA-4, i dati trasmessi tra l'emittente e il modulo crittografico, in cui è archiviata la chiave privata di autenticazione derivata da PIV, devono essere crittografati e contenere controlli di integrità dei dati.*
- *Il processo di emissione iniziale deve essere seguito per la chiave di un DPC scaduto o compromesso.*
- *Il processo di emissione iniziale deve essere seguito per la chiave di un DPC a LOA-4 su un nuovo token hardware.*
- *Quando si verifica una delle circostanze indicate di seguito, deve essere revocato il certificato di autenticazione PIV derivato oppure deve essere azzerato o distrutto il token contenente la chiave privata corrispondente:*
  1. *il token contenente la chiave privata corrispondente al DPC viene smarrito, rubato, danneggiato o compromesso;*
  2. *il token contenente la chiave privata corrispondente al DPC oppure il dispositivo mobile con un modulo crittografico incorporato sono trasferiti a un altro individuo;*
  3. *chi ha rilasciato la credenziale determina che il sottoscrittore non è più idoneo ad avere una tessera PIV (cioè, la tessera PIV è terminata);*
  4. *chi ha rilasciato la credenziale determina che il sottoscrittore non necessita più di un DPC, anche se la tessera PIV del sottoscrittore non è in scadenza.*
- *Se la tessera PIV del sottoscrittore viene riemessa a seguito della modifica del nome del sottoscrittore e il nome appare nel certificato di autenticazione PIV derivato, sarà necessario emettere anche un nuovo certificato di autenticazione PIV derivato con il nuovo nome.*

LINKAGE WITH PIV CARD REQUIREMENTS

- *Un emittente DPC emetterà un DPC a un richiedente solo se l'emittente DPC ha accesso alle informazioni della PIV Card del richiedente.*
- *L'emittente del DPC deve disporre di un meccanismo per verificare periodicamente con l'emittente della carta PIV per determinare se la carta PIV è stata disdetta o se le informazioni sulla persona che appariranno nel DPC (ad es. il nome) sono cambiate, poiché ciò richiederebbe la revoca o modifica del DPC.*
- *L'emittente del DPC dovrebbe verificare ogni 18 ore lo stato di cessazione. L'obbligo di verifica periodica può essere soddisfatto anche se:*
  1. *esiste un meccanismo di notifica tra l'emittente della carta PIV e l'emittente del DPC, oppure*
  2. *il record della PIV Card e il record del DPC sono archiviati nello stesso sistema e la cessazione della PIV Card attiva automaticamente la cessazione del DPC.*
- *L'emittente del DPC non deve basarsi esclusivamente sul monitoraggio dello stato di revoca del certificato di autenticazione PIV come mezzo per monitorare lo stato di cessazione della carta PIV.*
- *Devono essere impiegati metodi aggiuntivi per ottenere informazioni sulla PIV Card dall'emittente della PIV Card come:*

1. *se il DPC è emesso dalla stessa agenzia o emittente che ha emesso la PIV Card del sottoscrittore, l'emittente DPC può avere accesso diretto al database IDMS implementato dall'agenzia emittente che contiene le informazioni rilevanti del sottoscrittore;*
2. *quando l'emittente del DPC è diverso dall'emittente della carta PIV, possono essere applicati i seguenti meccanismi:*
   a. *il* BACKEND ATTRIBUTE EXCHANGE (BAE) *può essere interrogato per lo stato di terminazione della PIV Card, se è definito un attributo che fornisce queste informazioni e l'emittente della PIV Card mantiene questo attributo per il sottoscrittore. Il BAE può anche essere interrogato per altri attributi del sottoscrittore (ad esempio, nome) che possono apparire nel certificato di autenticazione PIV derivato;*
   b. *l'emittente del DPC notifica all'emittente il PIV originale quando viene creato un DPC. L'emittente della Carta PIV mantiene un elenco dei corrispondenti emittenti del DPC e invia a quest'ultimo una notifica quando la Carta PIV viene terminata o quando cambiano gli attributi relativi al titolare della carta. Tale notifica dovrebbe fornire la prova della ricezione e dell'integrità del messaggio.*
   c. *se viene implementato un* UNIFORM RELIABILITY AND REVOCATION SERVICE (URRS) *in conformità alla Sezione 3.7 del NIST Interagency Report (IR) 78177, l'emittente di un DPC può ottenere lo stato di cessazione della PIV Card del sottoscrittore attraverso l'*URRS.

TECHNICAL REQUIREMENTS

CERTIFICATE POLICIES

- *I certificati di autenticazione PIV Derivati devono essere emessi in base alla policy* ID-FPKI-COMMON-PIVAUTH-DERIVED-*hardware (LOA-4) o* ID-FPKI-COMMON-PIVAUTH-DERIVED *(LOA-3) della Policy sui certificati X.509.*
- *Il certificato di autenticazione PIV Derivato deve essere conforme al foglio di lavoro 10:* DERIVED PIV AUTHENTICATION CERTIFICATE PROFILE *trovato nel certificato X.509 e nel* CERTIFICATE REVOCATION LIST (CRL) EXTENSIONS PROFILE *per il* SHARED SERVICE PROVIDERS (SSP) PROGRAM.
- *La data di scadenza del certificato di* DERIVED PIV AUTHENTICATION *si basa sulla politica del certificato dell'emittente. Non è necessario allineare la data di scadenza del certificato di* DERIVED PIV AUTHENTICATION *con la data di scadenza del certificato di* PIV AUTHENTICATION *la scadenza della carta PIV; tuttavia, in molti casi l'allineamento delle date di scadenza semplificherà la gestione del ciclo di vita.*

CRYPTOGRAPHIC SPECIFICATIONS

- *L'algoritmo crittografico e i requisiti della dimensione della chiave per il certificato di* DERIVED PIV AUTHENTICATION *e la chiave privata sono gli stessi dei requisiti per il certificato di* PIV AUTHENTICATION *e la chiave privata, come specificato in NIST SP 800-78-4.9.*
- *Per i certificati di* PIV AUTHENTICATION *derivati emessi sotto* ID-FPKI-COMMON-PIVAUTH-DERIVED-HARDWARE (LOA-4), *la coppia di chiavi di* DERIVED PIV AUTHENTICATION *deve essere generata all'interno di un modulo crittografico hardware che è stato convalidato a FIPS 140-2 livello 2 o superiore che fornisce sicurezza fisica di livello 3 per proteggere la chiave privata di*

DERIVED PIV AUTHENTICATION *durante l'archiviazione e che non consente l'esportazione della chiave privata.*

- *Per i certificati di* DERIVED PIV AUTHENTICATION *emessi sotto* ID-FPKI-COMMON- PIVAUTH-DERIVED (LOA-3), *la coppia di chiavi di* DERIVED PIV AUTHENTICATION *deve essere generata all'interno di un modulo crittografico che è stato convalidato a FIPS 140-2 Livello 1 o superiore.*

CRYPTOGRAPHIC TOKEN TYPES

- *Removable (Non-Embedded) Hardware Cryptographic Tokens.*

1. *Un'applicazione PIV derivata deve essere installata sul token crittografico hardware. L'uso di questo modello di dati e della sua interfaccia supporta l'interoperabilità e garantisce che l'interfaccia DPC sia allineata con l'interfaccia della PIV Card.*
2. *Il fattore di forma supporta un elemento di sicurezza (Secure Element - SE), un componente crittografico a prova di manomissione che fornisce sicurezza e riservatezza.*
3. *Le unità di dati del protocollo di applicazione (*APPLICATION PROTOCOL DATA UNITS - APDU*) per l'interfaccia di comando del* DERIVED PIV APPLICATION *specificata nell'appendice B di NIST SP 800-157 sono trasportati all'elemento sicuro all'interno di ciascun fattore di forma tramite un protocollo di trasporto appropriato per quel fattore di forma.*
4. *Come descritto nell'Appendice B di NIST SP 800-157, la* DERIVED PIV APPLICATION *può includere chiavi private di gestione delle chiavi e firma digitale e i certificati corrispondenti oltre alla chiave privata di* DERIVED PIV AUTHENTICATION *e il relativo certificato.*
5. *SD Card con Cryptographic Module*
    1) *Un'applicazione* DERIVED PIV *può risiedere su un'implementazione di una scheda SD che include un elemento di sicurezza o un sistema di sicurezza a bordo.*
    2) *L'elemento di sicurezza utilizzato per l'applicazione* DERIVED PIV *deve supportare un'interfaccia con i comandi della card specificati nell'appendice B di NIST SP 800-157.*
6. *Removable* UICC (UNIVERSAL INTEGRATED CIRCUIT CARD) *con Cryptographic Module*
    1) LA DERIVED PIV APPLICATION *deve essere installata in un dominio di sicurezza separato dagli altri domini di sicurezza, dedicato al DPC, e sotto l'esplicito controllo dell'ente emittente.*
    2) *Gli* APDU (APPLICATION PROTOCOL DATA UNIT) *come specificato nell'appendice B di NIST SP 800-157 devono essere utilizzati con questo elemento di sicurezza contenente la PIV Derived Application.*
    3) *Un UICC utilizzato per ospitare un DPC deve implementare la* GLOBAL PLATFORM CARD SECURE ELEMENT CONFIGURATION.
7. *USB Token with Cryptographic Module*
    1. *Le implementazioni di token USB denominate* USB INTEGRATED CIRCUIT(S) CARD DEVICES (ICCD) *che contengono un elemento protetto integrato (*INTEGRATED CIRCUIT CARD O ICC) *sono adatte per l'emissione di DPC e sono conformi alla Classe di dispositivi* UNIVERSAL SERIAL BUS: SMART CARD ICCD SPECIFICATION *per* USB INTEGRATED CIRCUIT CARD DEVICES.

2. *Gli APDU per la* DERIVED PIV APPLICATION, *come specificato nell'appendice B di NIST SP 800-157, devono essere trasportati all'elemento sicuro utilizzando il tubo di comando* BULK-OUT *e le risposte devono essere ricevute dall'elemento sicuro utilizzando il comando* BULK-IN PIPE.
3. *I token USB con moduli crittografici che supportano un'applicazione PIV derivata devono inoltre essere conformi alle specifiche in NIST SP 800-9613 per il supporto APDU per lettori di schede a contatto.*

- *Embedded Cryptographic Tokens*
  1. *Un DPC e la sua chiave privata associata possono essere utilizzati in moduli crittografici incorporati in dispositivi mobili che possono essere sotto forma di modulo crittografico hardware, il quale è un componente del dispositivo mobile oppure sotto forma di modulo crittografico software che funziona nel dispositivo.*
  2. *DPC basati su software non possono essere emessi a LOA-4.*
  3. *L'approccio ibrido equivale all'archiviazione della chiave nell'hardware: il modulo crittografico software utilizza la chiave durante un'operazione di autenticazione, costituisce una soluzione LOA-3.*
  4. *Il modulo crittografico deve soddisfare i requisiti per i certificati emessi con* ID-FPKI-COMMON-PIVAUTH-DERIVED-HARDWARE *oppure* ID-FPKI-COMMON-PIVAUTH-DERIVED.
  5. *Questi stessi moduli crittografici possono contenere anche altre chiavi, come le chiavi private per la firma digitale e la gestione delle chiavi e i relativi certificati.*

ACTIVATION DATA

- *L'uso della chiave privata di* DERIVED PIV AUTHENTICATION *(oppure l'accesso alla chiave privata in chiaro o* wrapped*) deve essere bloccato prima dell'autenticazione del sottoscrittore basata su password.*
- *La password non deve essere facilmente indovinabile o identificabile individualmente.*
- *È previsto un meccanismo per bloccare l'uso della chiave privata di* DERIVED PIV AUTHENTICATION *dopo un numero di tentativi di attivazione consecutivi falliti, come stabilito dall'agenzia o ente.*
- *I meccanismi di limitazione (Throttling) possono essere utilizzati per limitare il numero di tentativi che possono essere eseguiti in un determinato periodo di tempo.*
- *Per i token incorporati (Embedded) a LOA-3, il meccanismo di autenticazione può essere implementato da meccanismi hardware o software al di fuori del confine del modulo crittografico, a condizione che la forza del meccanismo di autenticazione soddisfi i requisiti sopra specificati.*
- *Per i token rimovibili o i token incorporati a LOA-4, il meccanismo di autenticazione deve essere implementato e imposto dal modulo crittografico stesso.*
- *Quando la reimpostazione della password viene eseguita di persona presso la struttura dell'emittente o presso un chiosco incustodito gestito dall'emittente, la reimpostazione deve essere attuata attraverso uno dei seguenti processi:*
  1. *La PIV Card del Sottoscrittore deve essere utilizzata per autenticare il Sottoscrittore (tramite il meccanismo PKI-AUTH secondo la Sezione 6.2.3.1 di FIPS 201-2) prima della*

reimpostazione della password. L'emittente deve verificare che il DPC sia dello stesso Sottoscrittore che si è autenticato utilizzando la PIV Card.

2. *Deve essere eseguita una corrispondenza biometrica 1:1 rispetto al campione biometrico trattenuto durante l'emissione iniziale del DPC, un dato biometrico sulla carta PIV o dati biometrici archiviati nella catena di fiducia come specificato in FIPS 201-2. L'emittente deve verificare che il DPC sia per lo stesso Sottoscrittore per il quale è stata completata la corrispondenza biometrica*

- *Quando la reimpostazione della password viene eseguita in remoto, deve seguire i seguenti processi:*
  1. *La PIV Card del Sottoscrittore deve essere utilizzata per autenticare il Sottoscrittore (tramite il meccanismo di autenticazione PKI-AUTH secondo la Sezione 6.2.3.1 di FIPS 201-2) prima della reimpostazione della password.*
  2. *Se il ripristino avviene in una sessione separata dalla sessione in cui è stato completato il meccanismo di autenticazione PKI-AUTH, è necessario stabilire un collegamento forte (ad esempio, utilizzando un segreto temporaneo) tra le due sessioni.*
  3. *L'emittente verifica che il DPC sia dello stesso Sottoscrittore che si è autenticato con la PIV Card.*
  4. *La reimpostazione della password remota deve essere completata in una sessione protetta (ad es. utilizzando TLS).*
- *I token hardware rimovibili supportano la funzionalità di reimpostazione della password come da Appendice B di NIST SP 800-157 e il supporto per la reimpostazione della password non è richiesto in LOA-3 e le implementazioni possono invece scegliere di emettere un nuovo certificato dopo il processo di emissione iniziale se la password è dimenticato.*

2. USAGE SCENARIOS

Uno scenario di utilizzo è il modo pratico in cui gli utenti interagiscono con i componenti di un sistema e come funzionano insieme.

Il principio del "privilegio minimo", cioè "concedere agli utenti solo gli accessi di cui hanno bisogno per svolgere le loro funzioni ufficiali", richiede sia processi di autenticazione sia di autorizzazione.

Questa sezione descrive due scenari di utilizzo.

Nel primo scenario di utilizzo, sia la credenziale PIV sia il DPC sono emessi dallo stesso IDMS aziendale interno e la PKI di media garanzia.

Nel secondo scenario di utilizzo, la credenziale PIV è emessa da un provider di servizi condivisi attendibile esterno e il DPC è emesso da IDMS e PKI diversi.

Il resto di questa sezione descrive i seguenti scenari di utilizzo.

1. *Le credenziali PIV fornite dall'organizzazione e i DPC associati vengono emessi utilizzando un IDMS e una PKI aziendali (Paragrafo "Organization-Provisioned PIV Credentials Usage Scenario").*
2. *Le credenziali PIV fornite dal provider di servizi condivisi e i DPC associati vengono emessi utilizzando un IDMS e PKI diversi (Paragrafo "Shared Service Provider-Provisioned PIV Credentials Usage Scenario").*

ORGANIZATION-PROVISIONED PIV CREDENTIALS USAGE SCENARIO

Tradizionalmente, le organizzazioni forniscono credenziali PIV ai propri dipendenti, appaltatori e altri utenti di accesso logico in base al corrispondente record di identità del richiedente all'interno di un IDMS e PKI aziendale.

In questo scenario, l'organizzazione sta distribuendo dispositivi client moderni come smartphone, tablet e dispositivi di elaborazione generici ultraleggeri che non dispongono di lettori di PIV Card integrati o contactless.

Tuttavia, questi dispositivi forniscono un token hardware o software integrato che supporta i DPC.

Inoltre, l'IDMS aziendale e la PKI di media garanzia sono in grado di supportare l'emissione, l'uso, la manutenzione e la terminazione di DPC basati su X.509.

I DPC vengono utilizzati per autenticare e accedere a risorse remote ospitate all'interno di un data center in sede o in un cloud pubblico, nonché per firmare e crittografare la posta elettronica sul dispositivo client.

WORKFLOW

- *Un dipendente che ha superato il processo di verifica dell'identità PIV e possiede una credenziale PIV valida è idoneo per un DPC.*
- *Il dipendente necessita di un dispositivo mobile per lavorare.*
- *Viene ordinato il dispositivo mobile con un modulo crittografico e viene presentata una richiesta per il rilascio di un DPC all'autorità di approvazione.*
- *Possono essere rilasciati più DPC allo stesso dipendente sulla base della stessa PIV Card.*
- *Una volta che il dipendente ha ricevuto il dispositivo e la richiesta è stata approvata, il dipendente avvia il processo di rilascio.*
- *Se la credenziale emessa è a una LOA-4, il processo di emissione deve avvenire di persona e includere una corrispondenza biometrica con la credenziale PIV del dipendente.*
- *Il campione biometrico utilizzato per la verifica deve essere conservato per riferimento futuro.*
- *Il processo di emissione di una credenziale LOA-3 può avvenire in remoto e non richiede una corrispondenza biometrica.*
- *L'emissione di LOA-3 può essere avviata in remoto da un'entità gestita da un'Autorità di registrazione (RA) associata all'Autorità di Certificazione (CA) che rilascerà il DPC.*
- *Il processo di registrazione richiede comunicazioni protette tra tutti i componenti richiesti.*
- *Il Richiedente deve dimostrare di essere in possesso del certificato di Autenticazione Cliente PIV inserendo il PIN della propria Carta PIV.*
- *Poiché il dipendente non può utilizzare la PIV Card con il dispositivo mobile, il dipendente esegue questo passaggio da un computer noto e attendibile.*
- *Richiedendo l'uso del certificato di* PIV CLIENT AUTHENTICATION *durante la connessione al sistema di gestione delle credenziali (*CREDENTIAL MANAGEMENT SYSTEM CMS*), il server non solo autentica il richiedente, ma verifica anche che il richiedente sia ancora idoneo a possedere una credenziale PIV.*

- *Lo stato di revoca del certificato di autenticazione PIV del dipendente deve essere verificato anche sette giorni di calendario dopo il rilascio del DPC.*
- *Questo controllo impedisce l'emissione di DPC da una credenziale PIV rubata o compromessa.*
- *Dopo aver dimostrato l'idoneità del PIV, viene avviato il processo di rilascio del DPC*
- *Il CMS comunica con la CA DPC della PKI per richiedere il certificato di Derived PIV Client Authentication X.509 e i certificati di firma e crittografia opzionali.*
- *La CA emette i certificati richiesti e il CMS fornisce i certificati al dispositivo che richiede la credenziale.*
- *Il flusso di lavoro specifico per la raccolta delle credenziali sarà diverso a seconda delle scelte tecnologiche, delle politiche e dei processi specifici dell'organizzazione.*
- *Il dipendente potrebbe dover visitare una stazione di raccolta automatica, navigare in un sito Web mobile abilitato per TLS o eventualmente utilizzare un'applicazione mobile per raccogliere il DPC.*
- *Se il processo di raccolta richiede più di due sessioni interattive, è richiesto un identificatore di associazione del lavoro.*
- *L'identificatore dipende dal livello di garanzia che il DPC affermerà.*

La Figura 1 illustra un flusso di lavoro di registrazione e rilascio DPC fittizio.

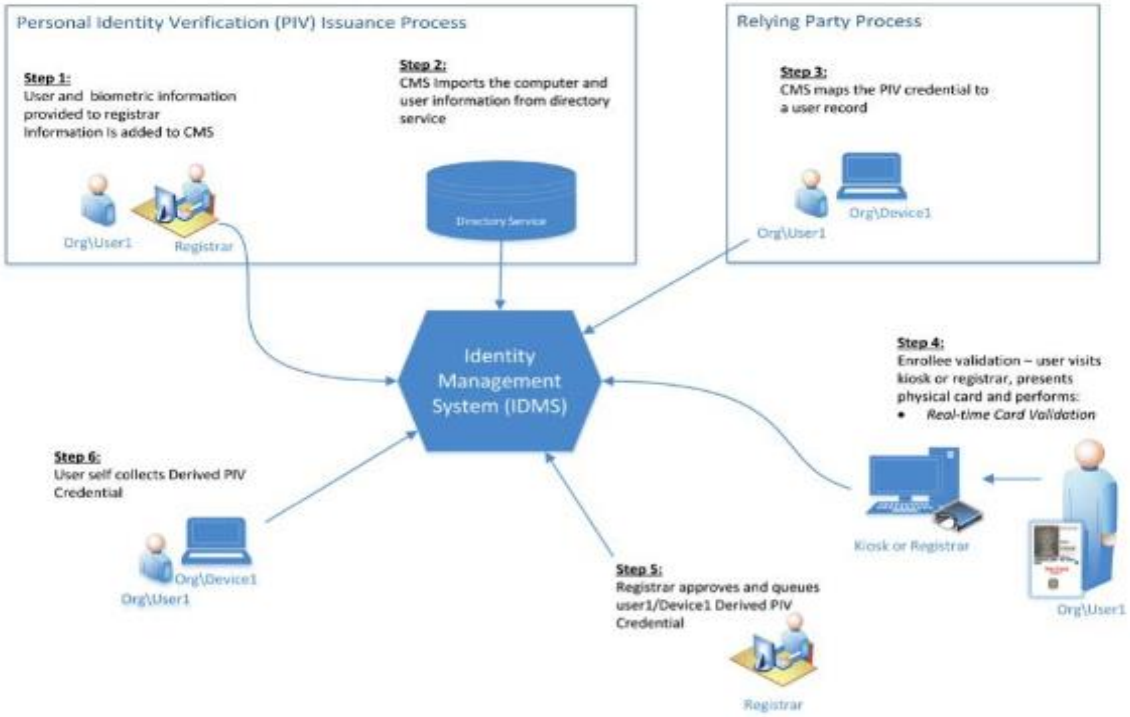

Figure 1: Enrollment and Issuance Workflow

LIFECYCLE MANAGEMENT

Il DPC è una credenziale separata dalla PIV Card, ma rimane valida solo se la PIV Card su cui si basava rimane non terminata.

Come qualsiasi altra credenziale utilizzata per l'autenticazione e l'autorizzazione, richiede funzioni di manutenzione e gestione del ciclo di vita.

Per tutta la durata del DPC di un Sottoscrittore possono verificarsi una serie di eventi che attiveranno una funzione di gestione del ciclo di vita.

Gli eventi che possono causare questi possono variare dalla modifica del nome di un Sottoscrittore alla compromissione di un DPC.

La tabella 1 descrive gli eventi che si verificano durante la vita di un DPC e le azioni corrispondenti richieste per affrontare questi eventi

Table 1: Lifecycle Management Functions

Event	Action Required
Cardholder name change and reissued PIV credential	Reissue DPC certificates
Credential is compromised	Issuance process
Credential expired / re-key	Issuance process
Token containing private key is lost	Zeroized/Destroyed/Revocation
Token containing private key is issued to different employee	Zeroized/Destroyed/Revocation
Subscriber no longer eligible to have PIV Card	Zeroized/Destroyed/Revocation
Subscriber no longer requires DPC	Zeroized/Destroyed/Revocation

La Figura 2 mostra la relazione tra il ciclo di vita per PIV e DPC, ed in particolare esiste solo un collegamento diretto per la riemissione e la terminazione della carta PIV.

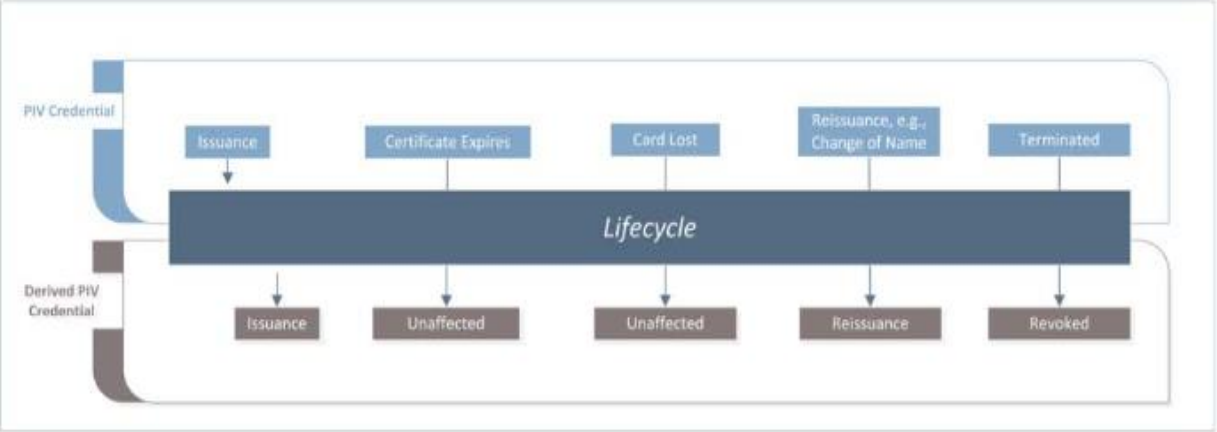

Figure 2: PIV and DPC Lifecycle

PROPOSED ARCHITECTURE

L'utilizzo di DPC richiede un'infrastruttura aziendale per supportare le attività di emissione, utilizzo, manutenzione e terminazione.

Questo scenario di utilizzo fa le seguenti ipotesi:

1. *l'organizzazione utilizza un IDMS aziendale;*
2. *l'organizzazione dispone di una PKI di media affidabilità consentita ai DPC emessi;*
3. *le risorse sono ospitate nel cloud e nel data center aziendale.*

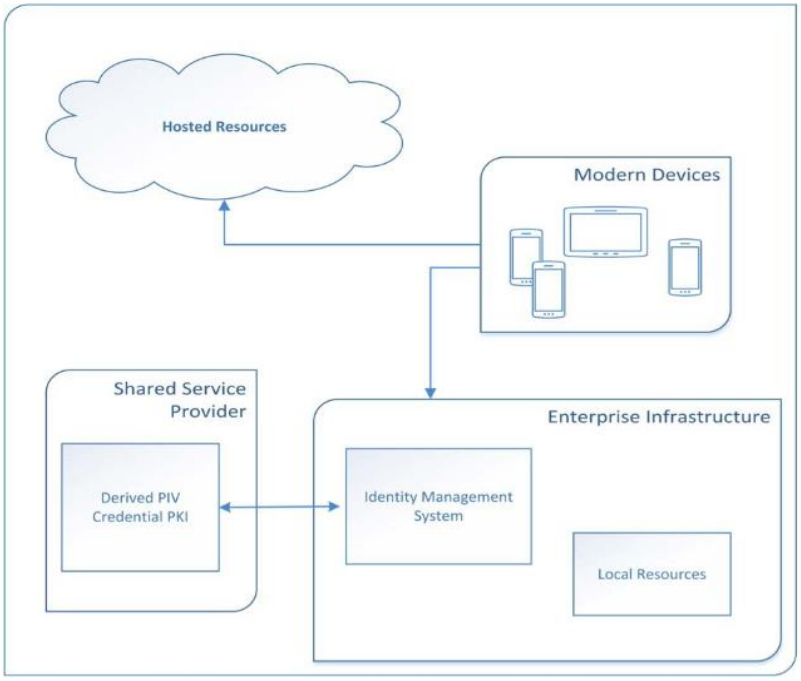

Figure 3: Scenario 1 Proposed Architecture

L'IDMS PIV interno dell'organizzazione è in grado di emettere e mantenere DPC su dispositivi moderni con fattori di forma che non supportano l'uso di una PIV Card fisica.

Queste nuove CA supporteranno l'emissione di DPC a diversi LOA in conformità con NIST SP 800-63-2.

Sarà necessaria un'infrastruttura aggiuntiva per supportare l'auto-raccolta dei DPC.

Risorse specifiche possono variare a seconda delle scelte tecnologiche, delle politiche e dei processi dell'organizzazione, ma potrebbero includere server applicativi aggiuntivi, applicazioni mobili, stazioni fisiche di raccolta automatica, ecc.

La Figura 3 riepiloga i componenti necessari per supportare lo scenario di utilizzo.

SHARED SERVICE PROVIDER-PROVISIONED PIV CREDENTIALS USAGE SCENARIO

In questo scenario, un'organizzazione desidera sfruttare le credenziali PIV fornite da SHARED SERVICE PROVIDER (SSP) *per generare DPC da utilizzare su vari dispositivi di elaborazione.*

Un sistema CMS locale e PKI supportano l'emissione, l'uso, la manutenzione e la terminazione dei DPC basati su X.509.

Prima che possa avvenire l'emissione dei DPC, l'IDMS locale deve verificare la validità delle credenziali PIV del dipendente.

L'obbligo di verificare la validità della PIV Card di un richiedente introduce la necessità per l'IDMS locale di disporre di un canale di comunicazione con il provider condiviso.

Questa comunicazione tra l'IDMS locale e il fornitore di servizi deve anche fornire un modo per notificare all'IDMS locale un evento di credenziale PIV come la terminazione di PIV.

In questo scenario di utilizzo, esiste un canale di comunicazione sicuro tra l'IDMS aziendale e l'IDMS della SSP.

La Figura 4 illustra l'infrastruttura aggiuntiva richiesta per l'emissione di DPC basati su un PIV emesso da SSP.

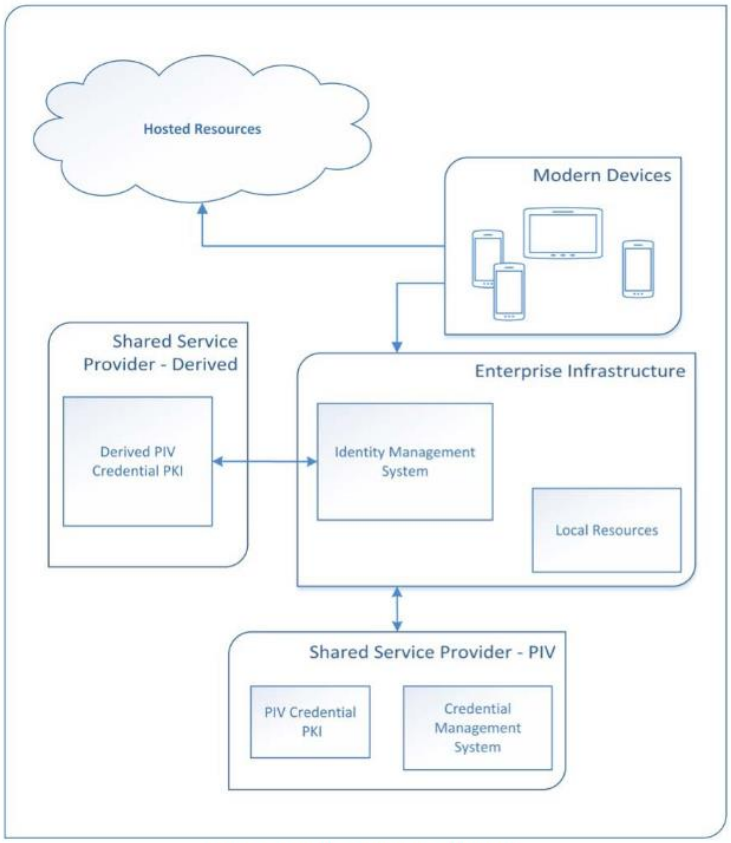

Figure 4: Scenario 2 Proposed Architecture

3. PROOF OF CONCEPT RESEARCH FOR ORGANIZATION-PROVISIONED PIV CREDENTIALS

Questa sezione spiega l'applicazione delle tecnologie Microsoft *e* Intercede *in conformità con NIST SP 800-157 per supportare lo scenario di utilizzo delle credenziali PIV fornite dall'organizzazione.*

Le tecnologie Microsoft *forniscono l'archivio di identità, i dispositivi mobili, l'infrastruttura di supporto e le applicazioni.*

Intercede MyID *è un sistema di gestione delle identità e delle credenziali conforme a FIPS 201 che aderisce alle specifiche NIST SP 800-157, ed è utilizzato come* CMS. (Nota: MyID® PIV is a software solution for federal agencies that issue and manage secure digital identities to federal employees using public key infrastructure (PKI)).

Il sistema di gestione delle credenziali Intercede MyID *fa parte dell'IDMS generale di cui al NIST SP 800-157.*

Questa sezione si concentra sull'emissione, l'utilizzo, la manutenzione e la cessazione delle credenziali LOA-3 in base alla guida degli SP NIST 800-157 e 800-63-2, nonché sulle tecnologie disponibili nel settore.

Entrambi i moduli crittografici hardware e software vengono utilizzati per proteggere la chiave privata del DPC.

ENTERPRISE INFRASTRUCTURE

È stato sviluppato un ambiente prototipo basato su cloud allo scopo di verificare l'interoperabilità della tecnologia per questa ricerca.

L'istanziazione di questo ambiente è stata configurata come tenant all'interno di Microsoft Azure Government (MAG) Infrastructure as a Service (IaaS).

L'uso dell'infrastruttura basata su cloud è stato scelto per il suo ambiente collaborativo ad alta disponibilità.

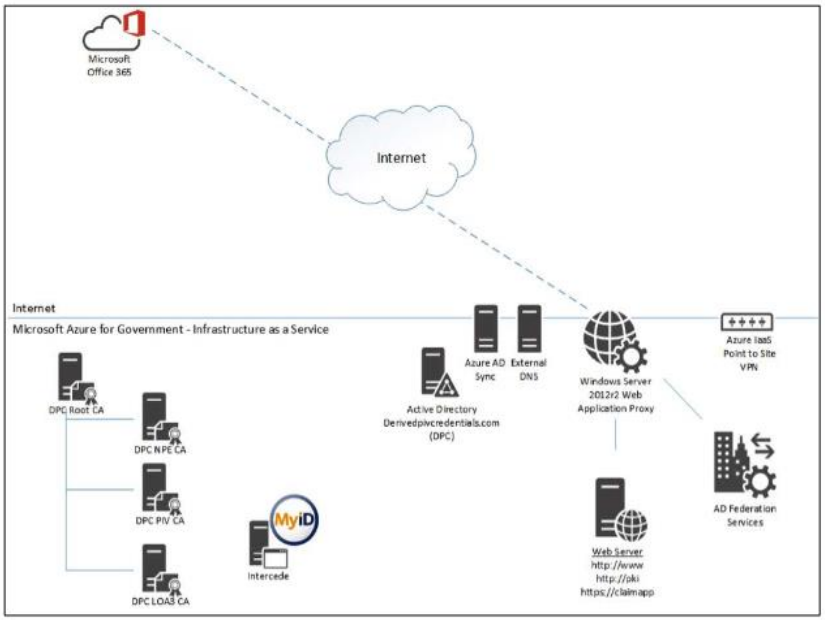

Figure 5: Architecture Core Components

Questo ambiente può essere distribuito in altri ambienti IaaS basati su cloud.

L'infrastruttura basata su cloud funge da dominio di identità per gli utenti a cui vengono emesse credenziali PIV e DPC.

Questi utenti si trovano all'interno del nome di dominio DerivedPIVCredentials.com (ad esempio, user1@DerivedPIVCredentials.com).

Le applicazioni a cui gli utenti accederanno sono i servizi Microsoft Office 365 Enterprise E3 basati su cloud.

L'utente si autentica su DerivedPIVCredentials.com Active Directory (AD) utilizzando il proprio DPC basato su X.509.

La Figura 5 descrive i componenti principali dell'architettura IaaS.

DERIVEDPIVCREDENTIALS.COM IDENTITIES

La Figura 6 illustra l'archivio di identità dell'utente (AD) utilizzato in questa ricerca.

MICROSOFT WINDOWS SERVER 2012 R2 ACTIVE DIRECTORY DOMAIN SERVICES (ADDS) *funge da archivio centrale di identità dell'utente ed è il centro di distribuzione delle chiavi* (KEY DISTRIBUTION CENTER - KDC) *per l'ambito Kerberos del dominio DerivedPIVCredentials.com.*

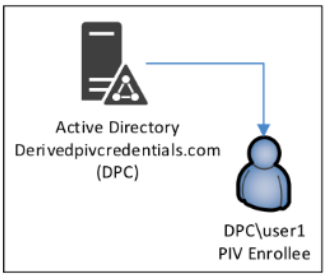

Figure 6: Active Directory User Identities

La comunicazione Kerberos è abilitata tra tutti i server all'interno della stessa rete virtuale IaaS (VNet) di Azure.

Questa rete non è esposta a Internet.

I sottoscrittori PIV e Derived PIV devono disporre di un account all'interno di questo dominio AD.

Il controller di dominio AD esegue il concatenamento X.509 e la validazione del certificato di autenticazione client PIV e Derived PIV utilizzato per l'autenticazione Kerberos.

Il ruolo ADDS è abilitato su due macchine virtuali MAG in esecuzione all'interno di un singolo Azure IaaS Cloud Service.

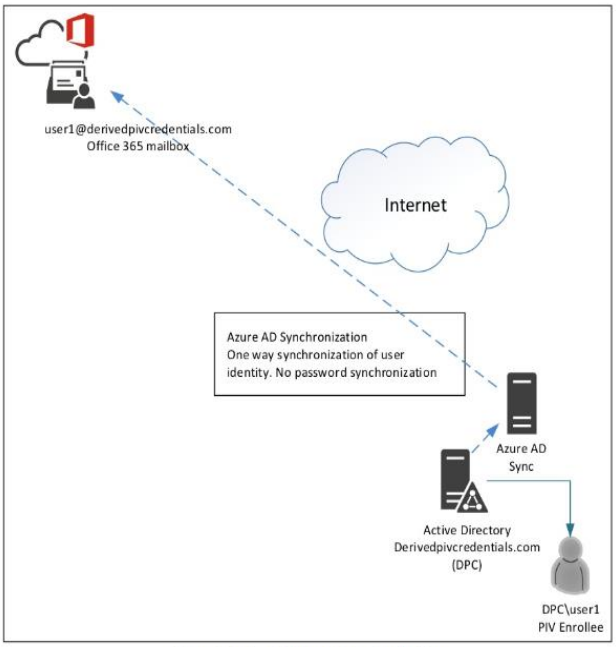

Figure 7: Office 365 Identity Synchronization

Le identità degli utenti vengono sincronizzate con il tenant di Azure AD associato tramite il motore di sincronizzazione di Azure Active Directory.

Solo gli attributi richiesti da Office 365 vengono sincronizzati con il tenant di Azure AD associato.

La figura 7 illustra la sincronizzazione delle identità con Office 365.

REMOTE SERVICES AND FEDERATION

La Figura 8 rappresenta il servizio remoto e l'architettura della federazione.

Microsoft Office 365, partner affidataria (Relying Party – RP), fornirà i servizi, a cui gli utenti mobili potranno accedere utilizzando le proprie credenziali basate su PIV e DPC X.509.

*NIST SP 800-157 afferma: "*Lo scopo delle credenziali PIV derivate è fornire servizi di autenticazione abilitati per PIV sul dispositivo mobile per autenticare il titolare della credenziale su sistemi remoti".

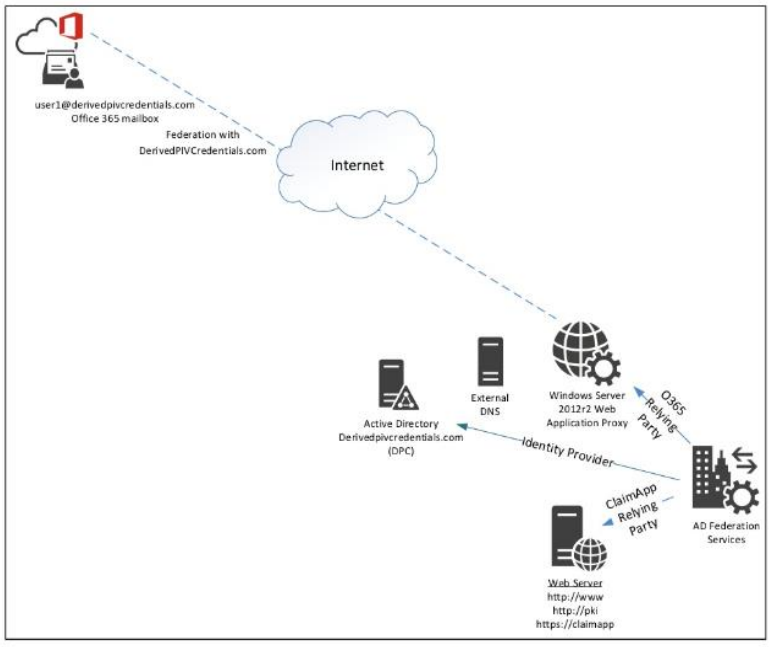

Figure 8: Federation Architecture

L'autenticazione (validazione delle credenziali X.509 e della mappatura degli account) avviene all'interno del dominio AD DerivedPIVCredentials.com basato su IaaS.

Il tenant di Office 365 di DerivedPIVCredentials.com sarà federato con ACTIVE DIRECTORY FEDERATION SERVICES (ADFS) *basato su IaaS che funge da provider di identità (IdP) per il dominio DerivedPIVCredentials.com.*

Il servizio di AZURE AD SYNCHRONIZATION *è configurato per non sincronizzare le password di AD degli utenti.*

DerivedPIVCredentials.com è registrato come federato.

Il servizio ADFS è fornito da due macchine virtuali Windows Server 2012R2 con il ruolo ADFS abilitato all'interno di un servizio cloud IaaS di Azure.

Queste macchine virtuali sono connesse alla stessa rete virtuale dei controller di dominio DerivedPIVCredentials.com poiché è necessaria la comunicazione Kerberos tra i server ADFS e ADDS.

La comunicazione esterna al servizio ADFS è fornita da due macchine virtuali Windows Server 2012R2 in un singolo servizio cloud Azure IaaS che esegue il ruolo ROUTING AND REMOTE ACCESS SERVICE (RRAS) *e* WEB APPLICATION PROXY (WAP).

Queste macchine virtuali non sono aggiunte a un dominio e sono collegate a una rete virtuale separata (VNET).

L'autenticazione X.509 al servizio IdP ADFS/WAP utilizza il metodo TLS CLIENT KEY EXCHANGE / CERTIFICATEVERIFY.

Il DerivedPIVCredentials.com Domain Name System (DNS) è configurato come "split DNS".

Le query sui nomi esterni sono inviate al server DNS esterno e le query DNS interne sono gestite dai server DNS integrati in ADDS.

Il DNS diviso è una tecnica comune utilizzata per rappresentare un singolo spazio dei nomi come indirizzi IP di origine diversi (interni o esterni) per le richieste del client che reindirizzano all'endpoint della federazione per l'autenticazione.

Un'applicazione di attestazioni di federazione di esempio è configurata sul "Web Server" (Internet Information Services, IIS 8).

Questa applicazione ASP.NET è associata al server ADFS come componente e visualizza il token SAML (SECURITY ASSERTION MARKUP LANGUAGE) *creato dal servizio ADFS nella pagina Web dell'utente.*

Questa applicazione verrà utilizzata per dimostrare la capacità di determinare quale credenziale l'utente autenticato con e fornire un livello di garanzia di autenticazione.

PKI

La PKI usata per supportare l'ambiente DerivedPIVCredentials.com, come mostrato nella Figura 9, si basa sul ruolo ADCS (Active Directory Certificate Services) di Windows Server 2012R2.

Tre CA emittenti vengono utilizzate per emettere certificati PIV, Derived PIV e non persona fisica (NON PERSON ENTITY - *NPE).*

Queste CA emittenti sono subordinate alla Root CA del DPC.

I CRL e i certificati richiesti per la creazione e la convalida della catena sono disponibili pubblicamente.

La DPC NPE CA è utilizzata per emettere certificati di entità finali non personali per supportare l'ambiente DerivedPIVCredentials.com (ad es. certificati del controller di dominio).

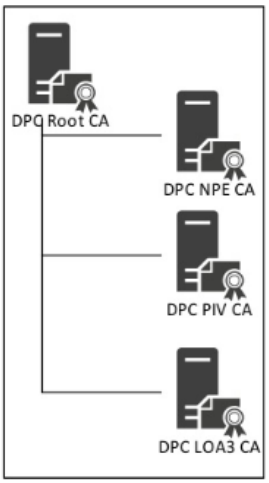

Figure 9: Public Key Infrastructure

La DPC PIV CA rilascia i certificati delle PIV Card.

La DPC LOA-3 CA emette i certificati del DPC per i DPC dei dispositivi mobili degli utenti.

Questo rapporto si concentra solo sull'emissione, l'utilizzo e la manutenzione di un LOA-3 DPC.

Il test OBJECT IDENTITY (OID), 2.16.840.1.101.3.2.1.48.17324, *è l'identificatore derivato da* ID-FPKI-COMMON-PIVAUTH *all'interno l'estensione* CERTIFICATEPOLICY *del certificato per identificare il certificato di Derived PIV Authentication.*

Il certificato End Entity Signature (cioè la firma digitale EES) sarà emesso per DPC LOA-3 CA per dimostrare le capacità di SECURE/MULTIPURPOSE INTERNET MAIL EXTENSIONS (S/MIME) *con il Sistema di posta elettronica di Office 365.*

Fare riferimento a X.509 Certificate and CERTIFICATE REVOCATION LIST (CRL) EXTENSIONS PROFILE *per il programma* SHARED SERVICE PROVIDERS (SSP) *per i formati dei certificati.*

MOBILE DEVICES

La Figura 11 rappresenta i vari dispositivi mobili utilizzati nella ricerca.

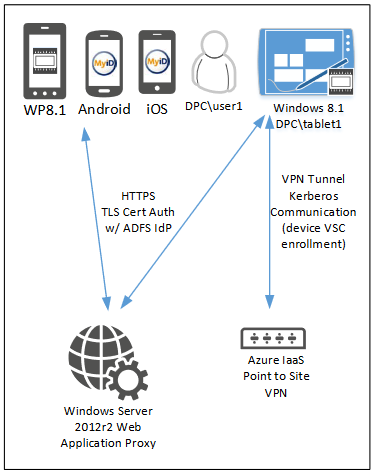

Figure 11: Mobile Devices

A partire da Windows 8, Microsoft ha introdotto la tecnologia Virtual Smart Card25 (VSC) per emulare la funzionalità delle tradizionali smart card basate su X.509.

La piattaforma Microsoft VSC utilizza il chip Trusted Platform Module26 (TPM) integrato nella maggior parte dei computer moderni.

Windows 10 include la tecnologia VSC e supporta tutte le funzionalità descritte in questo documento.

Microsoft, un partner di Fido Alliance, sta investendo in tecnologie (ad esempio Hello e Passport) che eliminano l'autenticazione basata su nome utente e password.

Queste tecnologie integreranno la tecnologia VSC nelle versioni future di Windows.

I DPC utilizzati in questa ricerca saranno Virtual Smart Card su Windows 8.1 e Piattaforme Windows Phone 8.1.

Un tablet che esegue il sistema operativo (OS) Windows 8.1 viene aggiunto al dominio DerivedPIVCredentials.com.

Il tablet Windows 8.1 aggiunto al dominio comunica con il dominio AD di DerivedPIVCredentials.com tramite la rete privata virtuale (VPN, punto a sito) di Azure IaaS.27 MyID eseguirà l'emissione di VSC tramite questo tunnel VPN per i dispositivi aggiunti al dominio.

Una VPN stabilita dimostrerà l'utilizzo di un DPC interno ai confini IT dell'organizzazione (ad esempio, accesso desktop).

Quando il tablet non è connesso tramite VPN a DerivedPIVCredentials.com, l'autenticazione e l'accesso verranno forniti tramite il servizio FS/WAP.

Quando la workstation non è in grado di eseguire comunicazioni basate su Kerberos con il dominio AD DerivedPIVCredentials.com, l'accesso desktop VSC utilizza la funzionalità di Windows delle credenziali memorizzate nella cache.

Microsoft Windows Phone 8.1 include il TPM e la tecnologia Windows 8 VSC.

Windows Phone è un contenitore DPC da utilizzare per l'autenticazione VPN, l'autenticazione ADFS X.509 (TLS CertificateVerify) e la firma digitale S/MIME.

L'applet Intercede MyID Windows Phone è necessaria per la registrazione, la manutenzione e la terminazione delle credenziali basate sul telefono.

L'applicazione Intercede MyID Identity Agent è disponibile in Windows Phone Store. Una volta che il DPC viene rilasciato al dispositivo Windows Phone 8.1, la smart card virtuale si comporta in modo simile a Windows 8.1 VSC e alla smart card fisica.

I dispositivi mobili Android v4.4.2 e iOS v7.x e versioni successive utilizzano MyID Identity Agent per fornire il modulo crittografico che genera e protegge il DPC.

La versione più recente di MyID Identity Agent deve essere installata dall'App Store ufficiale o dal Market Place della rispettiva piattaforma.

DERIVEDPIVCREDENTIALS.COM ENVIRONMENT

La Figura 12 mostra tutti i componenti dell'ambiente di test precedentemente descritti:

- *Identity store – AD*
- *DPC issuance – MyID*
- *PKI – ADCS*
- *Mobile devices – Windows, iOS, and Android*
- *Cloud-based resources – Office 365*
- *Federation – ADFS*

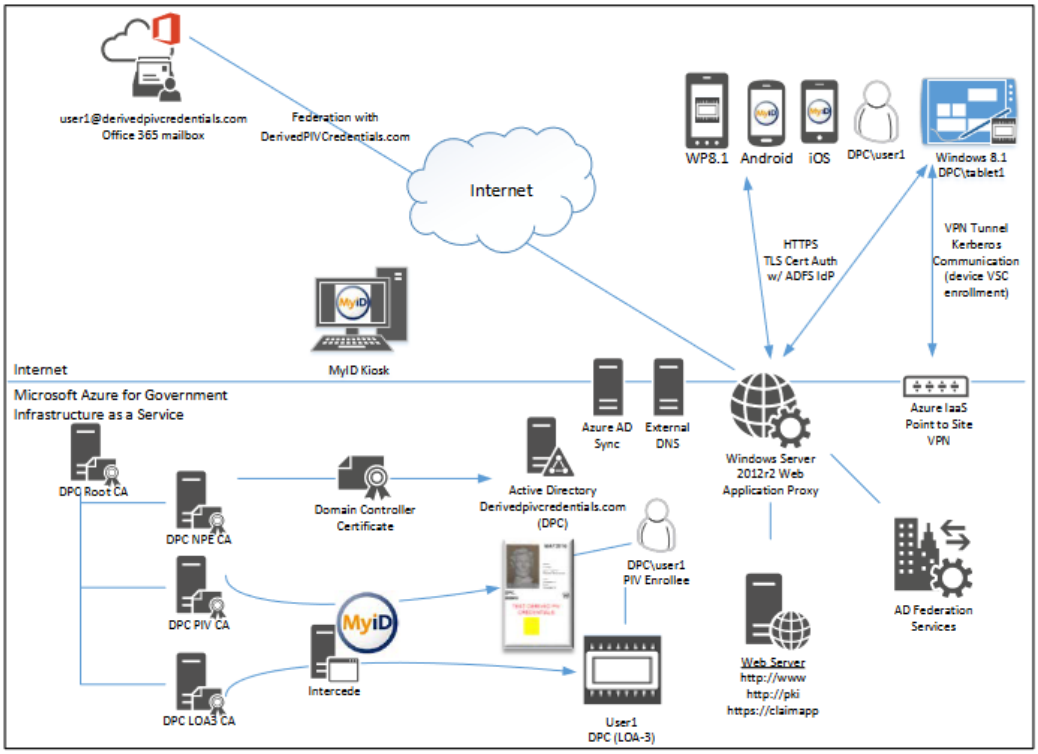

Figure 12: Complete Architecture of the research

IMPLEMENTATION CAPABILITIES

Questa sezione descrive i controlli tecnici che comprendono la soluzione dimostrata.

NIST SP 800-63-2 LOA

NIST SP 800-157 definisce i criteri di emissione del certificato in base al NIST SP 800-63-2 LOA come può affermare la credenziale.

I DPC possono affermare LOA-3 (id-fpki-common-pivAuth-derived, 2.16.840.1.101.3.2.1.3.40) e LOA-4 (id-fpki-common-pivAuth-derived-hardware, 2.16.840.1.101.3. 2.1.3.41).

NIST SP 800-63-2 raccomanda alle agenzie di selezionare le tecnologie di e-authentication appropriate dopo aver completato una valutazione dei rischi e aver mappato i rischi identificati al livello di garanzia richiesto in base a Office of Management and Budget (OMB) M-04-04 e E-Authentication Guidance.

La guida stabilisce requisiti tecnici specifici per ciascuno dei quattro livelli di garanzia.

X.509 CERTIFICATE AND CRL EXTENSIONS PROFILE FOR THE SSP PROGRAM

Il Federal Public Key Infrastructure Policy Authority's Derived PIV Authentication Certificate Profile (Worksheet 11: Derived PIV Authentication Certificate Profile) *è seguito per la creazione del profilo del certificato di autenticazione DPC.*

Le deviazioni dal profilo del certificato sono:

- *l'OID di test 2.16.840.1.101.3.2.1.48.173 è utilizzato per l'estensione* POLICYIDENTIFIER *per indicare* id-fpki-common-pivAuth-derived (LOA-3);
- *l'utente* DerivedPIVCredentials.com *AD* UserPrincipalName *del sottoscrittore è aggiunto come* otherName *all'interno dell'estensione* subjectAltName.

Il End Entity Signature Certificate Profile *è seguito per la creazione del profilo del certificato di DPC* End Entity Signature.

La deviazione dal profilo del certificato è:

- *Il* Secure Email OID 1.3.6.1.5.5.7.3.4 *è stato aggiunto a* extKeyUsage *per supportare la firma digitale* Outlook Web Access S/MIME.

IDENTITY PROOFING

NIST SP 800-157 afferma che la prova di identità e la registrazione utilizzate per il rilascio della carta PIV del richiedente possono essere applicate all'emissione del DPC del richiedente per non ripetere il processo di verifica dell'identità.

Il richiedente deve dimostrare il possesso e il controllo della PIV Card effettuando l'autenticazione con la credenziale del certificato di Autenticazione PIV.

Il modo in cui il richiedente si iscrive al DPC è un fattore nel determinare il livello di garanzia della credenziale.

Il MyID CMS può eseguire sia registrazioni LOA-4 (di persona, corrispondenza biometrica) sia LOA-3 (remote).

Questa ricerca dimostra le iscrizioni LOA-3.

TOKENS

NIST SP 800-63-2 definisce i seguenti token e i loro relativi livelli di garanzia:

➢ LEVEL 4 MULTI-FACTOR HARDWARE CRYPTOGRAPHIC TOKEN

- ✓ *Il modulo crittografico deve essere validato FIPS 140-2, livello 2 o superiore; con sicurezza fisica a FIPS 140-2 Livello 3 o superiore.*
- ✓ *Richiederà l'inserimento di una password, del PIN o di dati biometrici per attivare la chiave di autenticazione.*
- ✓ *Non consente l'esportazione delle chiavi di autenticazione.*

➢ LEVEL 3 MULTI-FACTOR SOFTWARE CRYPTOGRAPHIC TOKEN

- ✓ *Il modulo crittografico deve essere validato a FIPS 140-2 Livello 1 o superiore.*
- ✓ *Ogni autenticazione richiederà l'inserimento della password o di altri dati di attivazione e la copia non crittografata della chiave di autenticazione deve essere cancellata dopo ogni autenticazione.*

Table 2: NIST SP 800-63-2 LOA Mappings

NIST SP 800-63-2 Assurance Level	PIV Derived Authentication Certificate Policy	Cryptographic Token FIPS 140-2 Validation Level	Enrollment Requirements
LOA-3	id-fpki-common-pivAuth-derived	FIPS 140-2 Level 1	Remote enrollment allowed
LOA-4	id-fpki-common-pivAuth-derived-hardware	FIPS 140-2 Level 2 / Level 3 physical security	In-person enrollment required

Sono implementati solo token crittografici hardware e software LOA-3.

MICROSOFT VSC TECHNOLOGY

Microsoft Windows 8.1 VSC è un dispositivo crittografico basato su X.509 a più fattori.

Il TPM del sistema protegge la chiave crittografica del DPC che viene attivata tramite un secondo fattore di autenticazione (es. PIN).

L'autenticazione viene eseguita dimostrando il possesso del dispositivo e il controllo della chiave.

Tutte le funzioni di crittografia a chiave privata si verificano all'interno del TPM.

*La raccolta dei messaggi crittografici si verifica all'interno del provider di servizi di crittografia (*CRYPTOGRAPHIC SERVICE PROVIDER - CSP*) del sistema operativo.*

I VSC che utilizzano un TPM supportano tre principi di sicurezza principali:

1°. NON ESPORTABILITÀ: *poiché tutte le informazioni private su VSC sono crittografate utilizzando il TPM della macchina host, non possono essere utilizzate su una macchina diversa con un TPM diverso.*

Inoltre, i TPM sono progettati per essere a prova di manomissione e non esportabili, quindi un avversario non può decodificare un TPM identico o installare lo stesso su una macchina diversa.

2°. CRITTOGRAFIA ISOLATA: *i TPM forniscono le stesse proprietà della crittografia isolata offerta dalle smart card convenzionali, e queste sono utilizzate dai VSC.*

Quando tali proprietà sono utilizzate, le copie non crittografate delle chiavi private sono caricate solo all'interno del TPM e mai nella memoria accessibile dal sistema operativo.

Tutte le operazioni crittografiche con queste chiavi private avvengono all'interno del TPM.

3°. ANTI-HAMMERING: *se un utente inserisce un PIN in modo errato, il VSC risponde utilizzando la logica anti-hammering del TPM, che rifiuta ulteriori tentativi per un periodo di tempo invece di bloccare la carta.*

Questo è anche noto come blocco (lockout).

ADCS supporta l'attestazione TPM, che consente alla CA emittente di confermare che la chiave nella richiesta di certificato è protetta da un TPM noto.

Esistono tre metodi di attestazione del TPM:

1°. CREDENZIALI UTENTE: *la CA considera attendibile l'EKPub fornito dall'utente (la chiave pubblica della chiave di approvazione del TPM) come parte della richiesta del certificato e non è eseguita alcuna convalida rispetto alle credenziali di dominio del richiedente.*

2°. EKCERT: *la CA convalida la catena EKCert (il certificato associato la chiave TPM EKPub) fornita come parte della richiesta del certificato ed è membro di un elenco di catene EKCert consentite.*

3°. EKPUB: *la CA convalida che l'EKPub fornito come parte della richiesta del certificato sia membro di una lista di EKPub consentiti.*

I TPM implementano le funzionalità anti-martellamento per ridurre la minaccia di attacchi brutali per indovinare il PIN.

Il VSC si basa su questa funzionalità per proteggere ulteriormente le credenziali e implementerà il lockout TPM dopo cinque tentativi di PIN non riusciti.

Il periodo di blocco del TPM scadrà ma il VSC rimarrà bloccato. Il periodo di blocco del TPM dipende dall'implementazione della funzionalità da parte del produttore.

Sui dispositivi mobili che fanno parte del dominio, l'operatore MyID può ripristinare il blocco VSC eseguendo un CHALLENGE/RESPONSE PASSPHRASE EXCHANGE.

Altri servizi che utilizzano il TPM, ad esempio Bitlocker, *utilizzano un PIN diverso per consentire l'accesso alle chiavi protette da TPM. Pertanto, i PIN VSC e* Bitlocker *dovrebbero avere valori diversi.*

I dispositivi Windows a cui vengono emessi i DPC sono considerati token crittografici FIPS 140-2 Livello 1 validi se il TPM incorporato nel dispositivo è convalidato FIPS 140-2 Livello 1.

Il livello Microsoft CSP presenta il VSC allo stesso modo di una SMART CARD fisica. Ciò consente alle applicazioni compatibili con X.509 (ad es. Outlook, Internet Explorer) di utilizzare VSC senza driver o software aggiuntivi.

Entrambi i sistemi operativi Windows e Windows Phone utilizzano lo stesso CSP. Pertanto l'esperienza VSC su Windows e Windows Phone è la stessa.

ANDROID AND IOS DEVICE TOKENS

Il MyID Identity Agent fornisce il modulo crittografico che genera, protegge e interagisce con il DPC.

Il MyID Mobile SOFTWARE DEVELOPMENT KIT (SDK) *è incorporato nell'app MyID Identity Agent.*

Le chiavi private RSA per DPC sono generate all'interno di un modulo crittografico software FIPS 140-2 Level 1 (OpenSSL FIPS Object Module), il quale è fornito nell'app MyID Identity Agent.

I dati della chiave privata vengono conservati per l'archiviazione dall'app MyID Identity Agent in modo che solo le app firmate dallo stesso certificato di firma del codice possano accedere ai dati.

L'accesso alla chiave privata avviene tramite MyID Mobile SDK. I dati sono crittografati a riposo.

MyID Mobile SDK consente di utilizzare le chiavi private (ad es. per l'autenticazione) ed è integrato in applicazioni "derived credential enabled", come MyID Browser iOS, MyID Browser Android, MyID Mail iOS e MyID Mail Android.

Queste app sono firmate dal certificato di firma del codice corrispondente per consentire loro di accedere ai dati delle credenziali derivate.

Se terze parti desiderano sfruttare le credenziali derivate, l'SDK può essere messo a disposizione di terze parti in seguito al relativo accordo commerciale.

MyID Mobile SDK implementa la verifica della password/PIN, imponendo la verifica della password prima dell'attivazione della chiave privata di autenticazione PIV derivata. Dopo un numero di tentativi di verifica consecutivi falliti, la password e la chiave privata saranno bloccate.

4. RIFERIMENTI

1) NIST IR 8055 – Derived Personal Identity Verification (PIV) Credentials (DPC) Proof of Concept Research Resources
2) NIST SP 800-157 – Guidelines for Derived Personal Identity Verification (PIV) Credential