Identità Smart Card su Linux

Gianguido Piani

17 Marzo 2023

contenuti

- **installazione strumenti identità**
- identità digitale europea, eIDAS
- tool di accesso a smart card
- lettura certificati da smart card

cosa occorre

driver

programmi gestione

browser

moduli sicurezza

Le interfacce tra i vari moduli funzionali non sono esattamente definite e documentate, ma ci sono sovrapposizioni (non documentate).

Molti fornitori di soluzioni integrate, come per i documenti italiani o Bit4it per i lettori, offrono script di installazione completi. Questi portano però a incompatibilità tra più di una smartcard di tipo diverso sulla stessa piattaforma.

Ubuntu 22.04

- Ubuntu 22.04 contiene diverse utility di gestione smart card e interfacce lettori a contatto e NFC
- non sono necessari driver extra per i lettori (tocchiamo ferro)
- ma: perdita di usabilità causa snap
  - “*Unattended upgrade in progress during shutdown, please don’t turn off the computer*” (nessuna indicazione sul tempo richiesto)
- possono essere necessari
  - attivazione **pcscd daemon**
  - modulo ‘**opensc-pkcs11.so’** serve a diverse carte

Ubuntu 22.04, presupposti per identità digitale su Firefox

- Carta d’Identità Elettronica, Tessera Sanitaria post 2021 e Tessera Sanitaria ante 2021 richiedono **Firefox senza snap**

- Questi sistemi di identificazione su smartcard richiedono inoltre per Firefox un modulo crittografico da installare esplicitamente

modificare Firefox da snap a installazione regolare

- https://www.id.ee/en/article/ubuntu-id-software-installation-updating-and-removal/#removing-mozilla-firefox
- $ snap remove --purge firefox
- $ sudo apt remove --autoremove firefox
- $ sudo add-apt-repository ppa:mozillateam/ppa
- $ sudo nano /etc/apt/preferences.d/99mozillateamppa
  - Package: firefox*
  - Pin: release o=LP-PPA-mozillateam
  - Pin-Priority: 501
  -
  - Package: firefox*
  - Pin: release o=Ubuntu
  - Pin-Priority: -1
- $ sudo apt install -t 'o=LP-PPA-mozillateam' firefox
- $ sudo apt-get update && sudo apt-get upgrade

problemi con snap/Firefox, soluzioni

- https://onlinux.systems/guides/20220524_how-to-disable-and-remove-snap-on-ubuntu-2204
- https://askubuntu.com/questions/930593/how-to-disable-autorefresh-in-snap
- https://snapcraft.io/blog/hold-your-horses-i-mean-snaps-new-feature-lets-you-stop-snap-updates-for-as-long-as-you-need
- https://www.debugpoint.com/remove-snap-ubuntu/
- https://www.omgubuntu.co.uk/2022/04/how-to-install-firefox-deb-apt-ubuntu-22-04

uso di Firefox

- quando si usa Firefox insieme a un lettore di smart card, a contatto o NFC, è necessario prima inserire il lettore con la carta in uno slot USB e in seguito fare partire Firefox che così può riconoscere la presenza della carta e identificare il modulo necessario

pcscd daemon per lettore smart card

- se il lettore non è riconosciuto (lampada spenta sul lettore), attivare il servizio PCSCD (Personal Computer Smart Card Daemon)
    - **$ systemctl enable pcscd.socket**
    - **$ sudo systemctl start pcscd.socket**
    - **$ systemctl start pcscd.service**
- verifica con
    - **$ sudo service pcscd status**
- verificare inoltre
    - **$ dpkg -s openssl**
    - **$ dpkg -s libpcsclite1**

https://www.id.ee/en/article/diogidoc4-error-message-the-smartcard-pcsc-service-is-not-working/
https://www.tutorialspoint.com/unix_commands/pcscd.htm

Tessera Sanitaria AC 2014

- con Ubuntu 22.04 funziona direttamente
  - non è necessario installare driver per i dispositivi di lettura
  - occorre copiare il modulo '**opensc-pkcs11.so**' nelle cartelle
    - / usr/lib/x86_64-linux-gnu
    - / usr/lib/x86-64-linux-gnu/pkcs11

    e caricarlo in Firefox security devices

Tessera Sanitaria ST 2021, ST 2022 (1/2)

- scaricare una cartella compressa (77 MB) da
  - https://sistemats1.sanita.finanze.it/portale/elenco-driver-cittadini-modalita-accesso
  - https://sistemats1.sanita.finanze.it/portale/tessera-sanitaria-documenti-e-specifiche-tecniche
- dalla cartella è estratto il programma di installazione
  - istruzioni contenute in Readme.txt nel file zip scaricato. Eseguire con ./ (no sudo)
- viene installato PIN Manager (90 MB) nel sistema file utente
  - Programma attivato manualmente, non appare tra i programmi di sistema. Il programma reagisce alla presenza o cambio smart card sul lettore.
- dalla cartella ‘target/outerlibs’ copiare (sudo) i 5x moduli per l’accesso alla TS in
  - usr/lib/bit4id/outerlibs/* [è necessario creare la cartella bit4id]
- in Firefox è necessario caricare il modulo “libstpkcs11.so” (743 kB, totale cartella 5 MB) con un nome a scelta in

  Settings > Privacy & Security > Security Devices > Load

Tessera Sanitaria ST 2021, ST 2022 (2/2)

- il nuovo software Tessera Sanitaria funziona sia con lettore NFC, sia a contatti
- legge anche la TS AC2014

carta d’identità elettronica (1/3)

- il file di installazione (16 MB) si trova in
  - https://www.cartaidentita.interno.gov.it/fornitori-di-servizi/documentazione-middleware-cie/
  - file tipo .deb, aprire con **Software Install**
- viene installato il programma CIE ID (8 MB) per attivazione della carta, gestione del PIN e firma elettronica
  - cartella usr/share/CIEID
- lo script installa il modulo di accesso alla carta in
  - usr/local/lib/libcie-pkcs11.so
- in Firefox è necessario caricare il modulo “libcie-pkcs11.so” (36,4 MB) con un nome a scelta in
  - Settings > Privacy & Security > Security Devices > Load

carta d’identità elettronica (2/3)

- il programma di gestione CIE richiede **java**
  - $ **sudo apt install default-jre**
  - $ **java -version**
- è possibile utilizzare la CIE solo per login remoto, senza gestore CIE, copiando verso /homedirectory le cartelle nascoste .CIEID, .CIEPKI da altro sistema dove la CIE è già stata attivata
  - .CIEID contiene solo il file ‘**cieid.props**’
  - .CIEPKI contiene il file ‘**<12_cifre>.cache**’ e andrà a contenere log di lavoro

    <12_cifre> è il numero interno di identificazione della carta. E’ probabilmente possibile leggerlo con comandi in linea (non testato).

carta d’identità elettronica (3/3)

- la carta va inizialmente attivata con il programma CIE ID
  - occorre utilizzare le 8 cifre del PIN. Durante l’uso corrente sono sufficienti le 4 cifre della 2. parte.
- il programma CIE ID permette la gestione del PIN e firma elettronica
- il programma permette anche la firma elettronica (non qualificata) di documenti pdf, la funzionalità è intuitiva
- la CIE è codificata in modo proprietario e non è accessibile tramite le utility **opensc**, **pkcs11-tool**

carta d’identità elettronica

- https://developers.italia.it/it/cie/#dati-presenti-sulla-carta
- https://docs.italia.it/italia/cie/cie-manuale-tecnico-docs/it/master/overview.html

contenuti

- installazione strumenti identità
- **identità digitale europea, eIDAS**
- tool di accesso a smart card
- lettura certificati da smart card

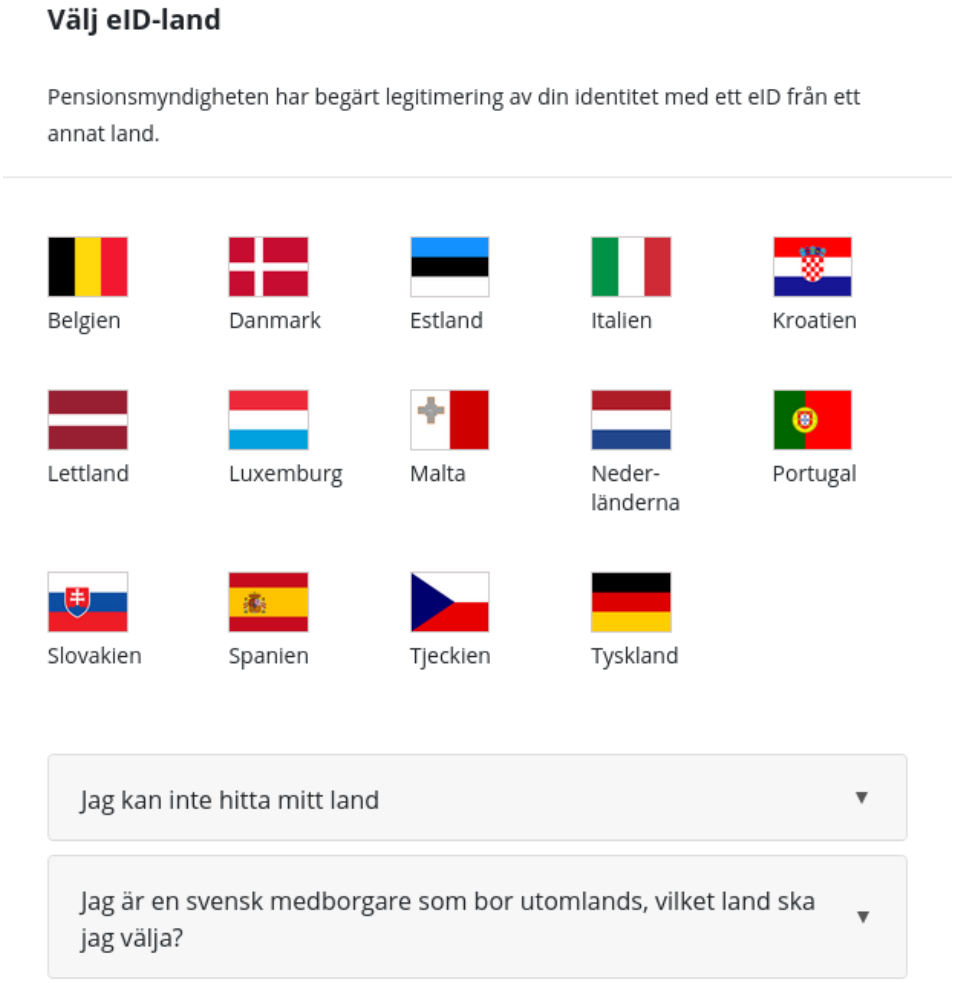
identità digitale in Europa

- in tutti i paesi europei con identità digitale questa è gestita dallo Stato
- eccezioni: Italia (SPID), Svezia
  - soluzioni basate sull'uso implicito o obbligatorio di uno smartphone
  - in Italia pubblicità estrema a favore di SPID
- il paese più flessibile con diversi canali è probabilmente la Germania, ma l'identità digitale è ancora indietro, pochi servizi, parzialmente manuali e quasi sempre basati su SMS "per verificare l'identità"
- Estonia paese più avanzato. Combinazione ben riuscita di semplicità, praticità, sicurezza
  - casella dedicata di corrispondenza
  - residenza virtuale
  - società locali, accesso mercati UE

identità digitale europea, eIDAS

- **electronic IDentification**, **Authentication** and trust **Services**
- EU Regulation 2014/910
  - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG
- eIDAS
  - login in siti esteri con credenziali e procedure nazionali
    - Italia unico paese a richiedere a ogni login l'accettazione della normativa "privacy"
  - ca 12 paesi, Italia molto avanzata
  - alcune incongruenze, ad esempio Svezia
- firma elettronica
  - c'è ancora parecchio da fare
  - concorrenza commerciale, es. Tessera Sanitaria vs. CamCom
- PEC europea
  - in fase di sviluppo, problemi con obbligo di PEC e costo

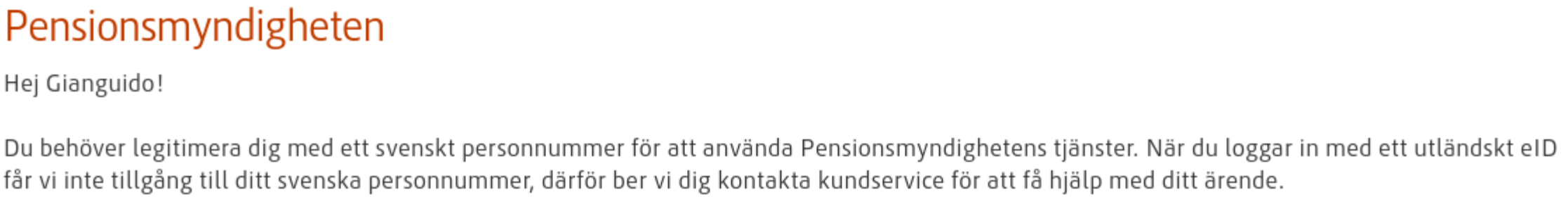
identità digitale europea, eIDAS



Esempio di login sul sito svedese delle pensioni. Dopo avere scelto il paese, ad es. Italia, si è rimandati alla procedura nazionale di login per quest'ultimo. Una volta verificata l'identità si torna al sito inizialmente richiesto.

Le procedure eIDAS basano l'identità su cognome, nome, data di nascita. Non sulla nazionalità, che può cambiare.

identità digitale europea, eIDAS


Pensionsmyndigheten

Hej Gianguido!

Du behöver legitimera dig med ett svenskt personnummer för att använda Pensionsmyndighetens tjänster. När du loggar in med ett utländskt eID får vi inte tillgång till ditt svenska personnummer, därför ber vi dig kontakta kundservice för att få hjälp med ditt ärende.

Il sito pensionistico svedese risponde di non potermi identificare perché non ho inserito il codice fiscale locale. Il problema è che neppure l'hanno chiesto!

eIDAS ha diverse criticità (una persona intelligente ci sarebbe arrivata subito):
- genera un nuovo codice fiscale secondo regole locali a ogni login. Un italiano che fa login su un sito spagnolo si vede così assegnato un C.F. spagnolo. Spetta alla Spagna verificare se ne ha già uno del paese oppure no.
- nei paesi nordici sono frequentissimi gli omonimi, vedi Sven Svensson in Svezia o Arne Rasmussen in Danimarca, magari nati lo stesso giorno nella stessa città. Il C.F. quindi non è più determinato univocamente dai dati anagrafici principali.
- in Germania un titolo tipo "Dr." può diventare parte del nome anagrafico. Fino a poco tempo fa le donne acquistavano il cognome del marito. Questo porta a ulteriori criticità.

identità digitale europea, eIDAS

La grande criticità di eIDAS è però che non fa riferimento a un hub centrale UE che da un lato verifica le identità presso i diversi paesi e dall'altro le conferma verso altri paesi.

Si basa invece su accordi bilaterali tra paesi con 27x26=702 possibili combinazioni di procedure di riconoscimento.

Vabbè che siamo "uniti nella diversità", ma qui stanno esagerando.

identità digitale in Europa, legislazione

- Regolamento (UE) n.910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica “eIDAS”
- Regolamento di esecuzione (UE) 2015/1502 della Commissione dell'8 settembre 2015 relativo alla definizione delle specifiche e procedure tecniche minime riguardanti i livelli di garanzia per i mezzi di identificazione elettronica
- Decisione di esecuzione (UE) 2015/1506 della Commissione dell'8 settembre 2015 che stabilisce le specifiche relative ai formati delle firme elettroniche avanzate e dei sigilli avanzati
- Direttiva (UE) 2015/2366 del Parlamento Europeo e del Consiglio del 25 novembre 2015 relativa ai servizi di pagamento nel mercato interno (PSD2)
- Regolamento (UE) 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (GDPR)
- Regolamento Delegato (UE) 2018/389 della Commissione del 27 novembre 2017 che integra la direttiva (UE) 2015/2366 riguardo le norme tecniche per l’autenticazione forte del cliente
- Regolamento (UE) 2019/1157 del Parlamento Europeo e del Consiglio del 20 giugno 2019 sul rafforzamento della sicurezza delle carte d'identità dei cittadini dell'Unione e dei titoli di soggiorno rilasciati ai cittadini dell'Unione e ai loro familiari

contenuti

- installazione strumenti identità
- identità digitale europea, eIDAS
- **tool di accesso a smart card**
- lettura certificati da smart card

opensc-tool

- tool generico per smart card, poche funzioni
  - https://manpages.org/opensc-tool

opensc-tool

- **--atr, -a**
  - answer to reset
- **--list-drivers, -D**
  - list all installed card drivers
- **--list-files, -f**
  - recursively list all files stored on card
- **--list-readers, -l**
  - list all configured readers

opensc-tool

- **--name, -n**
  - print the name of the inserted card (driver)
- **--serial**
  - print the card serial number (normally the ICCSN). Output is in hex byte format

pkcs11-tool

- utility per gestione e uso di token sicurezza PKCS #11
  - numerose funzioni
  - https://manpages.org/pkcs11-tool
  - https://www.systutorials.com/docs/linux/man/1-pkcs11-tool/
- PKCS #11

  “Personal Key Cryptographic Standard”. Definisce una API per dispositivi single-user con informazioni crittografiche quali certificati digitali e chiavi pubbliche. Questi dispositivi possono eseguire autonomamente funzioni crittografiche.

pkcs11-tool

- **--list-objects, -O**
  - display a list of objects
- **--read-object, -r**
  - get object attribute (use with **--type**)
  - **--type cert** restituisce un certificato in formato **.der**

pkcs15-tool

- PKCS #15: Cryptographic Token Information Format Standard
- utility per la gestione di strutture dati PKCS #15 su smart card e dispositivi simili di sicurezza, con numerose funzioni
  - https://manpages.org/pkcs15-tool
- con pkcs15-tool si possono presentare e leggere PIN, chiavi e certificati dal token. E' necessaria l'accesso preliminare con PIN.
- PKCS #15 definisce il formato delle credenziali crittografiche sui dispositivi. PKCS#15 cerca di unificare diverse soluzioni di crittografia che al momento ostacolano soluzioni di autenticazione e autorizzazione.
- https://stackoverflow.com/questions/33792095/what-does-it-mean-for-a-smart-card-to-be-pkcs15-compatible

pkcs15-tool

- **--list-objects, -O**
  - display a list of objects
-

contenuti

- installazione strumenti identità
- identità digitale europea, eIDAS
- tool di accesso a smart card
- **lettura certificati da smart card**

openssl

- preinstallato in ubuntu
  - https://www.openssl.org/docs/man3.0/
- utilizzato per funzioni relative ai certificati X.509, in particolare
  - conversione tra tipi di certificato
    - $ openssl x509 -inform DER -in cert.der -outform PEM > cert.pem
    - $ openssl x509 -in cert.pem -text > cert.txt
  - verifica della firma di un certificato rispetto ad altro certificato
- utilizzato in HTTPS

formati dei certificati

- X509 informazioni conosciute in punti predefiniti
- .der “Distinguished Encoding Rules”
  - certificato binario
- .pem “Privacy Enhanced Mail”

-----BEGIN CERTIFICATE-----
MIIH/TCCBeWgAwIBAgIQaBYE3/M08XHYCnNVmcFBcjANBgkqhkiG9w0BAQsFADBy
MQswCQYDVQQGEwJVUzEOMAwGA1UECAwFVGV4YXMxEDAOBgNVBAcMB0hvd
XNETAPBgNVBAoMCFNTTCBDb3JwMS4wLAYDVQQDDCVTU0wuY29tIEVWIFNTTC
BJbnRlmB1c4Kji6gOgA5uSUzaGmq/v4VncK5Ur+n9LbfnfLc28J5ft/GotinMyDk3iarF10Y
lqcOmeX1uFmKbdi/XorGlkCoMF3TDx8rmp9DBiB/SUzGV4YaGmq/v4VnBgNcK5Uw0B
-----END CERTIFICATE-----

- .crt, .txt Testo ASCII

lettura certificato via utility Linux

- lettura tramite **pkcs11-tool**
  - $ pkcs11-tool --read-object --id 01 --type cert --output-file cert.der
- conversione a testo con **openssl**
  - $ openssl x509 -in cert.der -text > cert.txt
- comando unico
  - $ pkcs11-tool --read-object --id 01 --type cert |
    openssl x509 -text > cert2.txt
- funziona con eeid, Tessera Sanitaria ST 2014, AC 2021, AC 2022
  - AC 2021, AC 2022 con contatto chip diretto

lettura certificato da Tessera Sanitaria AC 2021, 2022 (NFC)

- occorre identificare ID del certificato con **pkcs11-tool**
  - $ pkcs11-tool --list-objects --module <path>/outerlibs/libstpkcs11.so
  - il modulo è riportato come "ID: 434e5330”
- lettura tramite **pkcs11-tool**
  - $ pkcs11-tool --read-object --id 434e5330 --module <path>/outerlibs/libstpkcs11.so --type cert --output-file cert.der
- conversione in testo con **openssl**
  - $ openssl x509 -in cert.der -text > cert.txt
- comando unico
  - $ pkcs11-tool --read-object --id 434e5330 --module <path>/outerlibs/libstpkcs11.so --type cert | openssl x509 -text > cert3.txt

lettura certificato da Carta Identità Elettronica

- prova identificazione certificato con **pkcs11-tool**
  - $ pkcs11-tool --list-objects --module <path>/libcie-pkcs11.so
  - risposta errore java: not found
- prova con **opensc-tool**
  - $ opensc-tool -n
  - “Unsupported card”
  - cfr Tessera Sanitaria: "CNS card" (contatto), “Unsupported card” (NFC)

  - $ opensc-tool --serial
  - sc_card_ctl(*, SC_CARDCTL_GET_SERIALNR, *) failed [tutte le carte]

lettura certificato via Firefox

- lettura tramite Firefox (anche offline)
  - inserire smartcard, aprire Firefox
  - Settings > Privacy&Security > Certificates > View Certificates > [richiesta PIN] > Your Certificates > [select] > View > [print]
    - su carte ST2014 è richiesto PIN, ma non verificato
  - si può cliccare su Modulus e SHA-256 per espanderli prima della stampa
- funziona con Tessera Sanitaria, CIE
  - è necessario che sia presente il modulo relativo