eIDAS 2.0: stato dell'arte e prospettive per le Università

Giovanni Manca

8^ Conferenza organizzativa degli archivi delle Università italiane

12 aprile 2024

Agenda - 1

- Stato dell’arte di eIDAS 2.0.
- Il Portafoglio Europeo di Identità Digitale.
- La certificazione degli attributi.
- La gestione dei dispositivi per la firma e il sigillo «a distanza».

Agenda - 2

- Archiviazione elettronica.
- Registri elettronici.
- Protezione dei dati personali e cybersecurity.
- Criticità del regolamento eIDAS 2.0.

Stato dell’arte in eIDAS 2.0

Il lungo percorso di un compromesso

- Primo testo della Commissione in data 3 giugno 2021 per «*una proposta di Regolamento del Parlamento europeo e del Consiglio che modifica il regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione di un quadro per un'identità digitale europea*».
- Prima ratifica del Parlamento UE in data 16 marzo 2023.
- Approvazione nel trilogo in data 8 novembre 2023.
- Passaggio in Commissione parlamentare Industria, Ricerca ed Energia (ITRE) in data 28 novembre 2023 (poi approvato nella sessione del 7 dicembre 2023).
- Voto al testo del Parlamento 29 febbraio 2024 e approvazione del Consiglio il 15 marzo 2024. Pubblicazione in GUCE ed entrata in vigore dopo 20 giorni.

Le principali novità in eIDAS 2.0

- Struttura generale del regolamento analoga a quella attuale.
- Attuazione con 47 atti esecutivi.
- Nuovi servizi fiduciari di base, innovativi per l'Europa, come l'archiviazione elettronica di documenti e dati, l'attestazione elettronica degli attributi e i registri elettronici.
- Come già evidente nel titolo della proposta di regolamento il protagonista è EDIW (European Digital Identity Wallet).
- La crucialità di EDIW è confermata anche dal fatto che la quasi totalità della discussione istituzionale e degli *stakeholder* è concentrata sul Portafoglio.

I nuovi servizi fiduciari

- Il nuovo regolamento eIDAS introduce nuovi *Trust Services* (Servizi Fiduciari). Rimangono attivi quelli già stabiliti nel regolamento vigente.
- I nuovi servizi fiduciari sono:
  - ✓ «la attestazione elettronica degli attributi»;
  - ✓ «*l'archiviazione elettronica di documenti elettronici*»;
  - ✓ «la gestione dei dispositivi per la generazione di firme e sigilli da remoto»
  - ✓ «i registri elettronici».

Il Portafoglio Europeo di Identità Digitale (EDIW)

Definizione del Portafoglio UE

Nel testo consolidato di eIDAS 2.0 il wallet è definito come (nr. 42):

«*means an electronic identification means which allows the user to securely store, manage and validate person identification data and electronic attestations of attributes for the purpose of providing them to relying parties and other users of European Digital Identity Wallets, and to sign by means of qualified electronic signatures or to seal by means of qualified electronic seals*».

«*un mezzo di identificazione elettronica, che consente all'utente di conservare, gestire e convalidare in modo sicuro dati di identità personale e attestati elettronici di attributi al fine di fornirli alle parti facenti affidamento sulla certificazione e agli altri utenti dei portafogli europei di identità digitale, e di firmare mediante firme elettroniche qualificate o apporre sigilli mediante sigilli elettronici qualificati*».

Peculiarità del Portafoglio UE

- Il progetto è complesso tanto quanto politicamente seducente.
- I punti di maggiore complessità sono la certificazione del wallet, la modernità dei dispositivi fisici di supporto e *l'onboarding* delle informazioni utente. Sul wallet la firma elettronica qualificata deve essere a disposizione dell'utente in modo gratuito (ma solo per i cittadini e non per scopi professionali).
- Il documento di riferimento tecnico è stato pubblicato per la prima volta il 10 febbraio 2023 ed è referenziato come ARF (Architecture Reference Framework).
- E' giunto alle versione 1.3 e con esso è stato reso disponibile il software Android e iOS in *open source*.

Scenario per il Portafoglio UE

- Accesso sicuro, affidabile e senza soluzione di continuità ai servizi pubblici e privati in modo transnazionale per persone fisiche e giuridiche.
- L'utente del Portafoglio deve avere il pieno controllo dei propri dati.
- Ciascun Stato membro deve fornire almeno un Portafoglio entro 24 mesi dall'entrata in vigore di atti esecutivi emessi in conformità al regolamento.
- Sono stabilite regole per l'emissione e la gestione del Portafoglio.

Generalità su EDIW - 1

- Il Portafoglio Europeo di Identità Digitale è il vero protagonista della trasformazione ed evoluzione digitale comunitaria.

- La maggior parte del dibattito sia istituzionale, che pubblico e dei portatori di interesse si è focalizzato su questo tema.

- Le funzionalità del Portafoglio sono numerose a partire delle interazione che questo deve fare per operare in conformità alla normativa e alle specifiche tecniche uniche a livello comunitario.

- Le criticità di sicurezza e protezione dei dati personali sono numerose e molte di esse saranno risolte con evoluzioni di quanto già diffuso e ben noto. ENISA (L'Agenzia UE per la sicurezza cibernetica) ha un ruolo esplicitamente stabilito in eIDAS 2.0 che si coordina con il

Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza»).

Generalità su eDIW - 2

- La definizione, mostrata in precedenza, mette in evidenza il rapporto stretto tra l'identità personale e le interazioni con il mondo esterno al portafoglio.
- Sono altresì evidenti le criticità di sicurezza per la memorizzazione locale dei dati, la gestione delle copie di sicurezza anche per il ripristino dell'ambiente operativo.
- Il principio chiave è quello del completo controllo dei dati del portafoglio in entrambi le direzioni dei flussi operativi. Due portafogli possono interagire direttamente tra loro.
- Per specificare il contesto di utilizzo dell'identità digitale, EDIW interagisce e utilizza in modo coordinato gli attestati elettronici degli attributi.

Le basi legali

- Articolo 5 bis del nuovo regolamento.

- *«Al fine di garantire che tutte le persone fisiche e giuridiche nell'Unione abbiano un accesso transfrontaliero sicuro, affidabile e senza soluzione di continuità a servizi pubblici e privati, mantenendo nel contempo il pieno controllo dei loro dati, ciascuno Stato membro fornisce almeno un portafoglio europeo di identità digitale entro 24 mesi dall'entrata in vigore degli atti di esecuzione di cui al paragrafo 23 e all'articolo 5 quater, paragrafo 6».*

- I portafogli sono emessi dagli Stati membri, su incarico di uno Stato membro, indipendentemente da uno Stato membro pur essendo riconosciuti da quest'ultimo. Il codice sorgente dei portafogli deve caratterizzato da una licenza *open source*.

- Sono stabilite anche, in estremo dettaglio, le attività consentite all'utente con il portafoglio. Tali attività devono essere «*user friendly*» in altre parole intuitive, trasparenti e tracciabili da qust'ultimo.

Principali funzionalità - 1

- L’utente deve disporre di un cruscotto che contiene le transazioni effettuate tramite il Portafoglio.
- Deve essere disponibile il tracciamento delle transazioni tramite un cruscotto che aggrega le informazioni per l’utente.
- Deve essere offerto **gratuitamente** a tutti gli utenti non professionali, il servizio di firma elettronica qualificata.
- Deve essere disponibile lo scaricamento dei propri dati, degli attestati elettronici degli attributi e le configurazioni.
- Deve essere esercitato il diritto di portabilità dei dati tra portafogli dello stesso utente.

Principali funzionalità - 2

- *Per la protezione dei dati personali:*
  - *«chiedere facilmente che una una parte che fa affidamento sulla certificazione cancelli dei dati personali a norma dell'articolo 17 del Regolamento (UE) 2016/679»;*
  - *«segnalare facilmente la parte facente affidamento sulla certificazione all'autorità nazionale di protezione dei dati competente qualora sia ricevuta una richiesta di dati personali presumibilmente illecita o sospetta.»*

Principali funzionalità - 3

- Vengono stabilite regole, puntuali e anche un po’ ripetitive, sui diritti dell’utente e sulle regole di sicurezza e protezione dei dati personali nell’ambito degli utilizzi del portafoglio o di più portafogli nella titolarità dello stesso utente.

- Viene stabilito il diritto di delega per l’uso del portafoglio ad una altra persona fisica e giuridica. Questo diritto deve essere attuato con uno specifico meccanismo d’uso.

- Altre funzionalità gratuite sono stabilite per la verifica di autenticità e validità di portafogli, attestazioni di attributi e anche sull’identità delle parti facenti affidamento.

- Deve essere disponibile il supporto tecnico al portafoglio che deve essere disponibile in modo semplice.

- Il portafoglio è progettato in modalità «security-by-design» e supporta la sicurezza necessaria allo «state-of-the-art».

Principali funzionalità - 4

- L’uso del portafoglio non è obbligatorio.

- «*L'uso dei portafogli europei di identità digitale è facoltativo. L'accesso ai servizi pubblici e privati e al mercato del lavoro nonché la libertà d'impresa non sono in alcun modo limitati o resi svantaggiosi per le persone fisiche o giuridiche che non utilizzano i portafogli europei di identità digitale. Resta possibile accedere ai servizi pubblici e privati con altri mezzi di identificazione e autenticazione esistenti*».

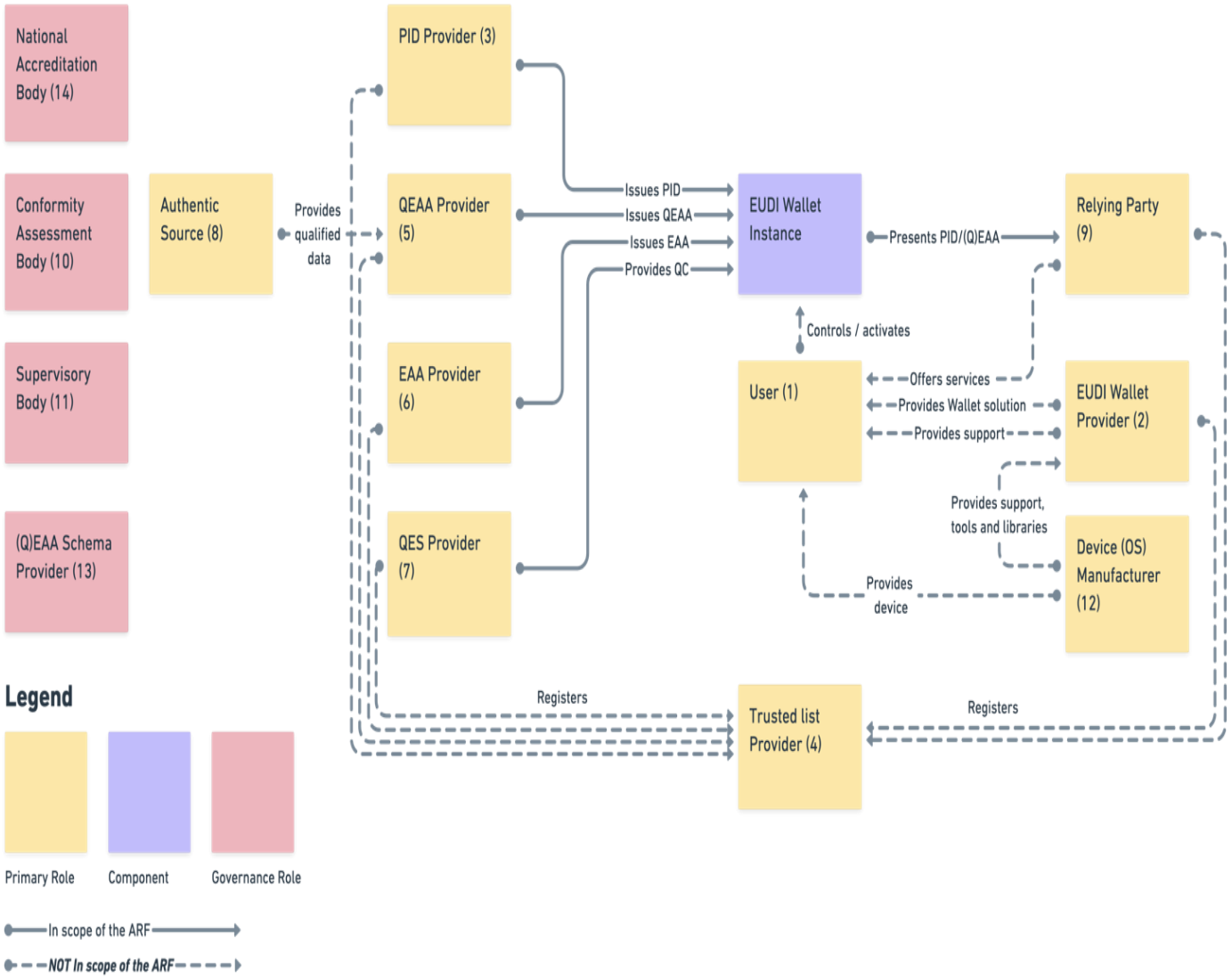
- L’architettura di riferimento del portafoglio è stabilità attraverso un Board consultivo e un documento che evolve allo stato dell’arte demominato Architecture and Reference Framework (ARF).

- Il titolo completo è «*The Common Union Toolbox for a Coordinated Approach Towards a European Digital Identity Framework – The European Digital Identity Wallet Architecture and Reference Framework*».

Altri aspetti generali sul portafoglio

- Certificazione dei portafogli.
- Pubblicazione della lista dei portafogli certificati.
- Regole per le parti facenti affidamento sulla certificazione dei portafogli. Queste sono note al sistema e devono autenticarsi per svolgere il loro ruolo.
- Regole per la violazione della sicurezza dei portafogli. Compromissione, violazione dei dati (*data breach*) e aspetti analoghi. La Commissione pubblica «senza indugio» i portafogli ritirati perché l'incidente di sicurezza non ha trovato rimedio.

Il portafoglio nell'ARF



1. *Utenti finali del EDIW*
2. *Prestatori del EDIW*
3. *Prestatori di Dati Identificativi della Persona (PID)*
4. *Prestatori di elenchi pubblici di fiducia*
5. *Prestatori di attestazioni elettroniche di attributi qualificate (QEEA)*
6. *Prestatori di attestazioni elettroniche di attributi non qualificate (EEA)*
7. *Prestatori di certificati qualificati e non qualificati per le firme e i sigilli elettronici*
8. *Fonti autentiche*
9. *Parti facenti affidamento*
10. *Organismi per la valutazione della conformità (CAB)*
11. *Organismi di vigilanza*
12. *Fabbricanti di dispositivi e fornitori dei sottosistemi relativi*
13. *Prestatori degli schemi (Q)EAA*
14. *Organismi nazionali di accreditamento*

L’attestazione elettronica degli attributi

Attestazione attributi

- L’attributo è una caratteristica, qualità, diritto o autorizzazione di una persona fisica o giuridica o di un oggetto.
- L’attestato elettronico di attributi è un attestato in forma elettronica che consente l’autenticazione di attributi.
- L’attestato elettronico può essere qualificato, in quanto servizio fiduciario, ad esso è dedicato l’allegato V dello schema di regolamento.
- La fonte autentica è «*un archivio o un sistema, tenuto sotto la responsabilità di un organismo del settore pubblico o di un soggetto privato, che contiene e fornisce gli attributi relativi a una persona fisica o giuridica o a un oggetto e che è considerato una fonte primaria di tali informazioni o la cui autenticità è riconosciuta conformemente al diritto dell'Unione o nazionale, inclusa la prassi amministrativa;*».

La gestione dei dispositivi per la firma e il sigillo «a distanza»

Il servizio di gestione «remota»

- La firma remota diffusissima in Italia diventa un servizio fiduciario esplicito in eIDAS 2.0.

- Lo diventa con l'articolo (completamente nuovo) 29 bis. Requisiti relativi ai servizi qualificati per la gestione di dispositivi per la creazione di una elettronica a distanza (traduzione ufficiale per «*remote*»).

- In questo caso la parte sicurezza amplia il suo perimetro perché viene specificato l'obbligo di certificazione per il dispositivo e si stabiliscono anche regole per la continuità operativa e il recupero dai disastri del servizio.

- Il Portafoglio è progettato per interagire in modo significativo con i servizi di firma remota (a distanza).

Archiviazione elettronica

Il servizio di archiviazione elettronica

- L’archiviazione elettronica è «*un servizio che consente la ricezione, la conservazione, la consultazione e la cancellazione di dati elettronici e documenti elettronici al fine di garantire la durabilità e leggibilità nonché di preservarne l'integrità, la riservatezza e la prova dell'origine per tutto il periodo di conservazione*».

- Il servizio può, ovviamente, essere qualificato sulla base di quanto stabilito nell’articolo 45 octies.

- Quanto stabilito nell’articolato dello schema di regolamento eIDAS 2.0 è la descrizione ampliata della definizione e ulteriori dettagli funzionali e operativi vengono rinviati ad atti esecutivi che conterranno gli standard da applicare per questo servizio.

- Alla data la specifica di riferimento per le misure di sicurezza è la ETSI TS 119 511.

Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques

Le regole UE per l’archiviazione - 1

Articolo 45 decies

Effetti giuridici dei servizi di archiviazione elettronica

1. Ai dati elettronici e ai documenti elettronici conservati mediante un servizio di archiviazione elettronica non vengono negati gli effetti giuridici né l'ammissibilità come prova in procedimenti giudiziari per il solo motivo della loro forma elettronica o perché non sono conservati mediante un servizio di archiviazione elettronica qualificato.

2. I dati elettronici e i documenti elettronici conservati mediante un servizio di archiviazione elettronica qualificato godono della presunzione della loro integrità e della correttezza della loro origine per la durata del periodo di conservazione da parte del prestatore di servizi fiduciari qualificato.

Le regole UE per l'archiviazione - 2

Articolo 45 undecies

Requisiti per i servizi di archiviazione elettronica qualificata

1. I servizi di archiviazione elettronica qualificati soddisfano i requisiti seguenti:

a) sono forniti da prestatori di servizi fiduciari qualificati

b) utilizzano procedure e tecnologie in grado di garantire la durabilità e la leggibilità dei dati elettronici e dei documenti elettronici oltre il periodo di validità tecnologica e almeno per tutto il periodo di conservazione legale o contrattuale, preservandone nel contempo l'integrità e l'esattezza dell'origine;

c) assicurano che tali dati elettronici e tali documenti elettronici siano conservati in modo tale da essere protetti dal rischio di perdita e alterazione, ad eccezione delle modifiche riguardanti il loro supporto o il loro formato elettronico;

d) consentono alle parti autorizzate facenti affidamento sulla certificazione di ricevere una relazione in un modo automatizzato in cui si conferma che i dati elettronici e i documenti elettronici consultati da un archivio elettronico qualificato godono della presunzione di integrità dei dati dall'inizio del periodo di conservazione fino al momento della consultazione.

La relazione di cui alla lettera d) del primo comma è fornita in modo affidabile ed efficiente e reca la firma elettronica qualificata o il sigillo elettronico qualificato del prestatore del servizio di archiviazione elettronica qualificato.

2. Entro ... [12 mesi dalla data di entrata in vigore del presente regolamento modificativo] la Commissione, mediante atti di esecuzione, stabilisce un elenco di norme di riferimento e, se necessario, stabilisce specifiche e procedure applicabili ai servizi di archiviazione elettronica qualificati. Si presume che i requisiti dei servizi di archiviazione elettronica qualificati siano rispettati ove un servizio di archiviazione elettronica qualificato sia conforme a tali norme, specifiche e procedure. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Registri elettronici

Generalità sui registri elettronici - 1

Definizione

- *52) "registro elettronico", «una sequenza di registrazioni di dati elettronici che garantisce l'integrità di tali registrazioni e l'accuratezza dell'ordine cronologico di tali registrazioni;».*

- *53) "registro elettronico qualificato", un registro elettronico fornito da un prestatore di servizi fiduciari qualificato e che soddisfa i requisiti di cui all'articolo 45 terdecies".*

- Non sono citate le parole «decentralizzato o «distribuito».

- Certamente non possono essere esclusi i concetti di blockchain o smart contract.

Generalità sui registri elettronici - 2

SEZIONE 11

REGISTRI ELETTRONICI

Articolo 45 duodecies

Effetti giuridici dei registri elettronici

1. A un registro elettronico non sono negati gli effetti giuridici né l'ammissibilità come prova in procedimenti giudiziari per il solo motivo della sua forma elettronica o perché non soddisfa i requisiti per i registri elettronici qualificati.

2. *Le registrazioni di dati contenute in* un registro elettronico qualificato godono della presunzione del loro ordine cronologico sequenziale *univoco e accurato e della loro integrità*.

Generalità sui registri elettronici - 3

Articolo 45 terdecies

Requisiti per i registri elettronici qualificatii

1. I registri elettronici qualificati soddisfano i requisiti seguenti:

   a) sono creati *e gestiti* da uno o più prestatori di servizi fiduciari qualificati;
   b) stabiliscono l'origine delle registrazioni di dati nel registro;
   c) garantiscono l'ordine cronologico sequenziale *univoco delle registrazioni di* dati nel registro;
   d) registrano i dati in modo tale che sia possibile individuare immediatamente qualsiasi successiva modifica degli stessi, *garantendone l'integrità nel tempo*.

2. Si presume che i requisiti di cui al paragrafo 1 siano stati rispettati ove un registro elettronico sia conforme alle norme, *alle specifiche e alle procedure* di cui al paragrafo 3.

3. Entro ... [12 mesi dalla data di entrata in vigore del presente regolamento modificativo] la Commissione, mediante atti di esecuzione, *stabilisce un elenco di norme di riferimento e, se necessario, stabilisce specifiche e procedure applicabili ai requisiti di cui al paragrafo 1* del presente articolo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.";

Criticità del regolamento eIDAS 2.0

Tutto bello ?

- La sfida del Portafoglio Europeo di Identità Digitale è di alto livello.
- Quanti portafogli pubblici e privati ci saranno ?
- La protezione dei dati personali sarà percepito in modo sereno o il Portafoglio sarà considerato un «super controllore» ?
- I Portafogli pubblici come si sosterranno economicamente ?
- Quanto sarà complesso il passaggio tra SPID e il Portafoglio italiano/europeo.
- La CIE è pronta a reggere il peso di un «dopo SPID» ? (Se ci sarà un «dopo SPID»).

Conclusioni

- Il Portafoglio Europeo di Identità Digitale è un progetto cruciale per lo sviluppo dei sistemi e dei servizi digitali nella società dell'informazione e della comunicazione.

- Lo schema di regolamento eIDAS II che modifica il regolamento vigente stabilisce nuove e numerose regole sul tema. Lo scenario operativo è altamente critico per la protezione dei dati personali e anche molto complesso per i numerosissimi flussi di informazioni coinvolti.

- Le istituzioni europee stanno lavorando alacremente e con tempistiche molto veloci.

- Il sistema sarà un successo se il portafoglio sarà percepito come un strumento vicino al cittadino e non come la base del «grande fratello». In altre parole la parola **fiducia** dovrà essere la parola chiave di questo nuovo e cruciale ecosistema.

Fine del Seminario

DOMANDE ???

Contatto del relatore:

Giovanni Manca
e-mail: mncgnn59@gmail.com