Privacy e sicurezza informatica secondo i nuovi standard ISO/IEC

Banche e Sicurezza 2015, ABI

Roma, 5 giugno 2015

UNINFO

Agenda

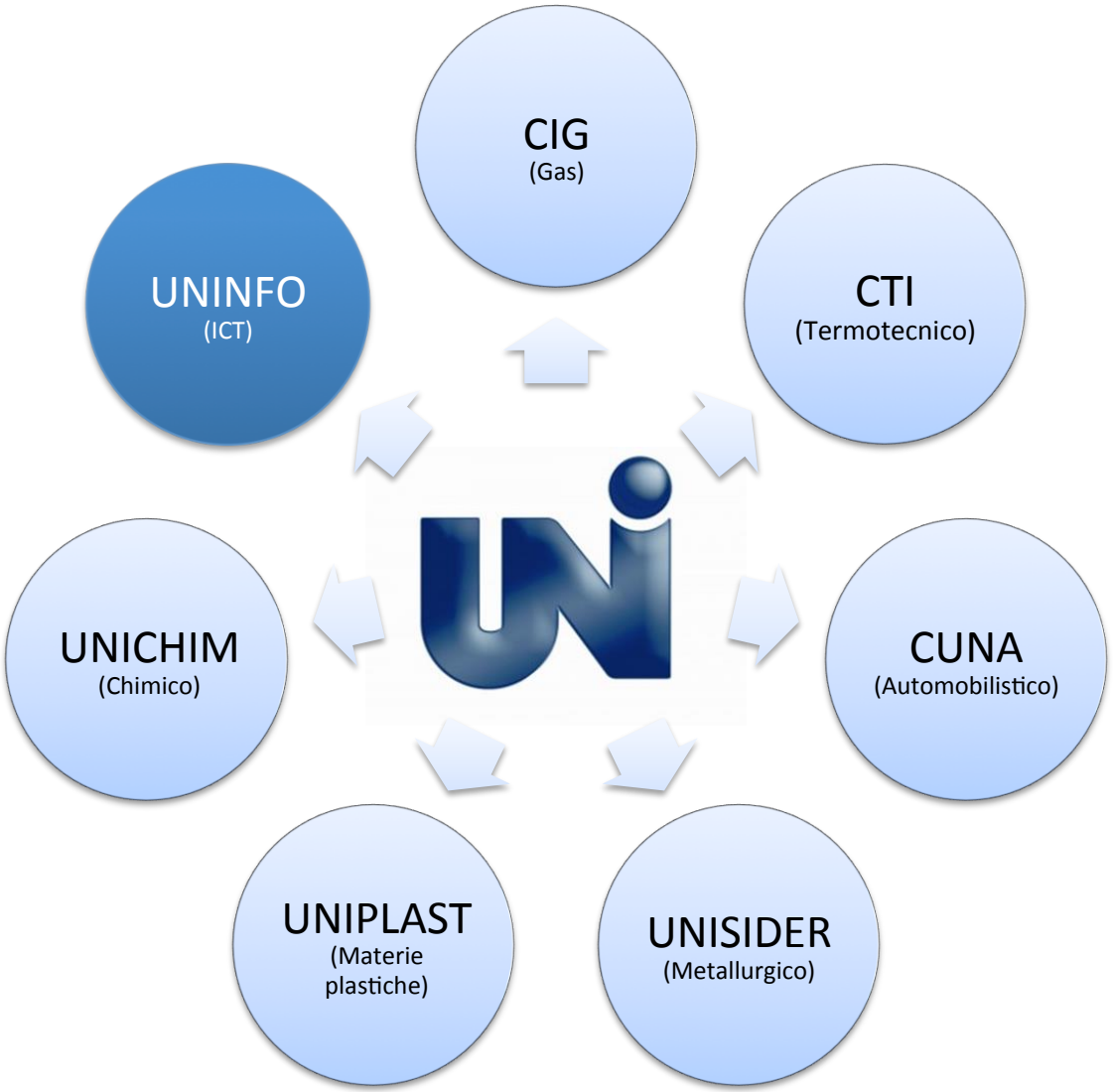
- UNINFO ed SC27
- Privacy e Security
- ISO/IEC 29100: Privacy Framework
- ISO/IEC 29134: Privacy Impact Assessment
- ISO/IEC 29151: Controlli
- Profili professionali
- Altre attività nazionali ed europee

Relatore

Fabio GUASCONI

- ✓ Direttivo di **UNINFO**
- ✓ Presidente del ISO/IEC JTC1 SC27 UNINFO
- ✓ Direttivo **CLUSIT**
- ✓ CISA, CISM, PCI-QSA, ITIL, ISFS, Lead Auditor 27001 & 9001
- ✓ Partner e co-founder **BL4CKSWAN** S.r.l

Normazione in Italia: ecosistema UNI



UNI è l'Ente Nazionale Italiano di Unificazione, più colloquialmente detto anche "Ente Italiano di Normazione"

Ha 7 enti federati che si occupano di tematiche verticali

UNINFO

UNINFO

"**UNINFO** è una libera Associazione a carattere tecnico-scientifico e divulgativo senza fine di lucro (diretto o indiretto) che si prefigge di promuovere, realizzare e diffondere la normazione tecnica nel settore delle tecnologie dell'informazione e delle comunicazioni (in breve ICT) e delle loro applicazioni, sia a livello nazionale che europeo ed internazionale."

Estratto dallo Statuto UNINFO

UNINFO

Settori di attività di UNINFO

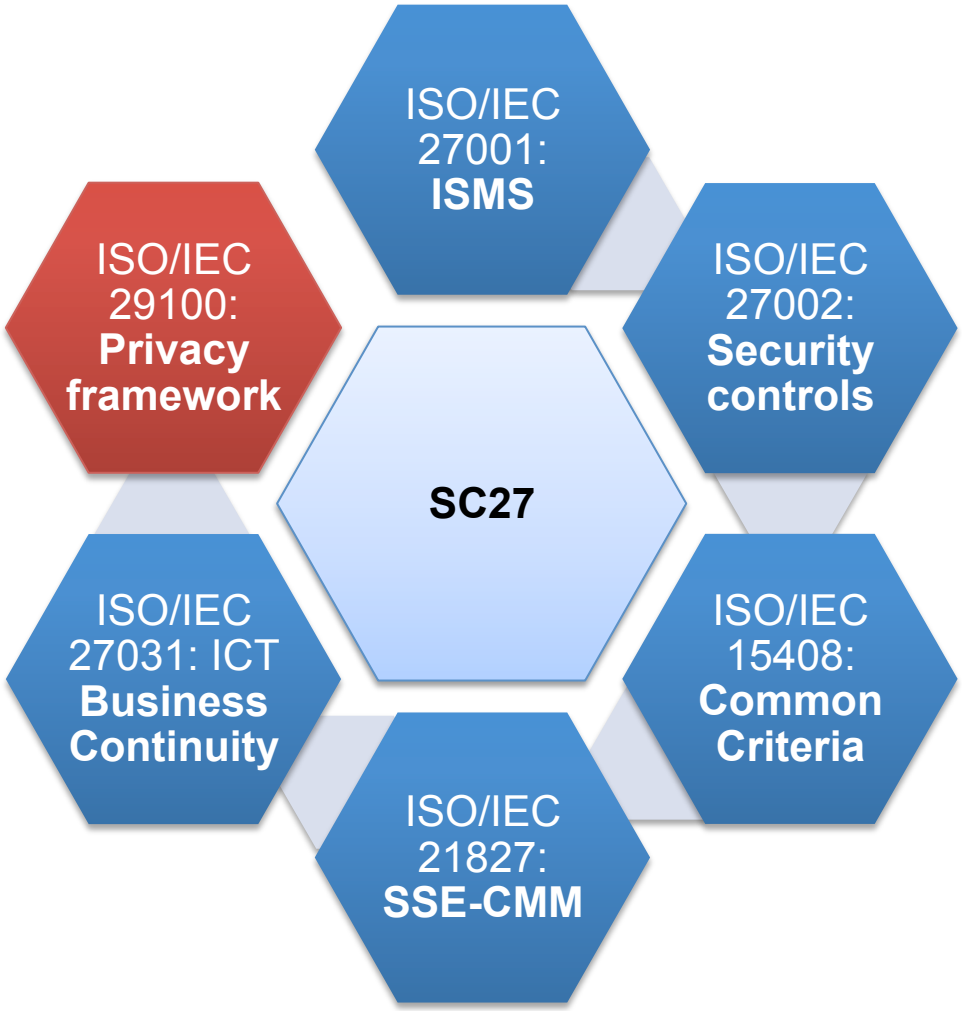
Sicurezza

Informatica, SC27

UNINFO

Norme e WG di ISO/IEC JTC1 SC27

WG5: aspetti di sicurezza di gestione delle identità, biometria e privacy



WG1: sistemi di gestione per la sicurezza delle informazioni, controlli, accreditamento, certificazione e audit, governance

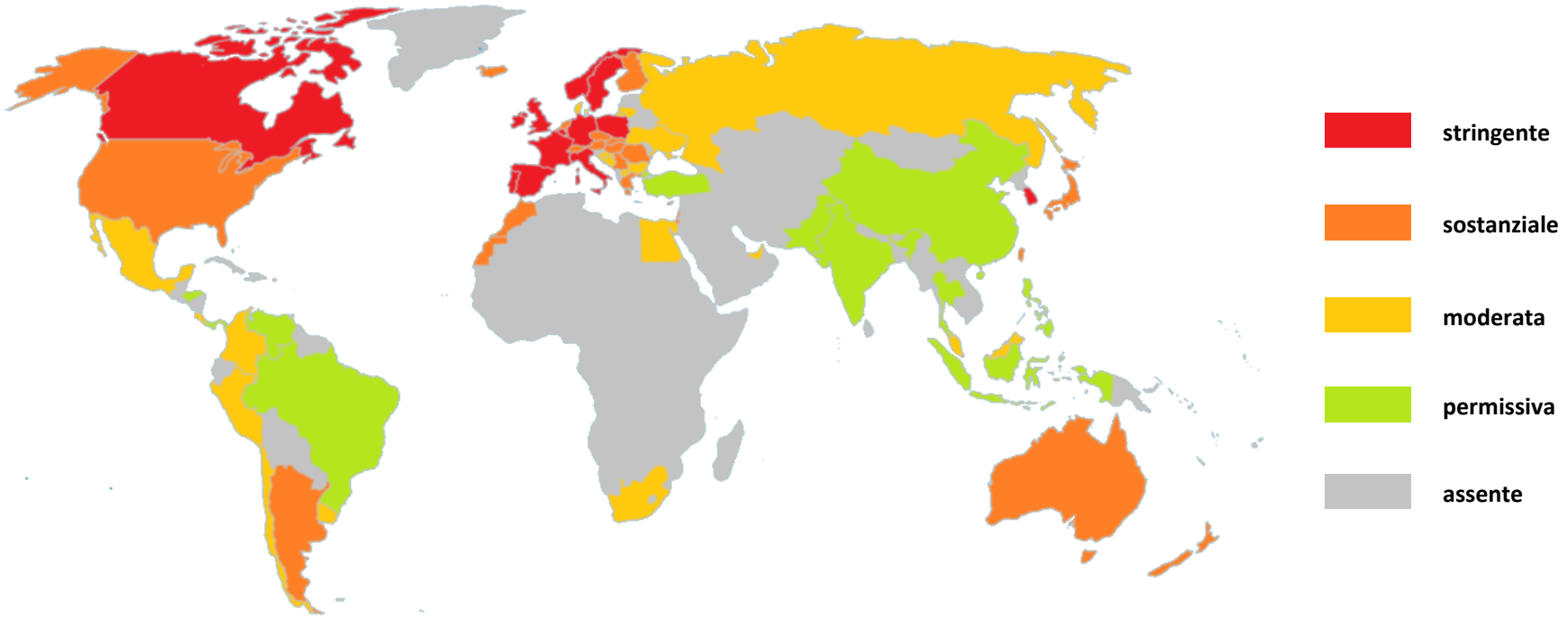
WG4: servizi di sicurezza collegati all'attuazione dei sistemi di gestione per la sicurezza delle informazioni

WG3 criteri, metodologie e procedure per la valutazione, il test e la specifica della sicurezza

UNINFO

Perché normare in ambito Privacy

Molti paesi del mondo hanno le loro leggi in materia, con diversi livelli di permissività

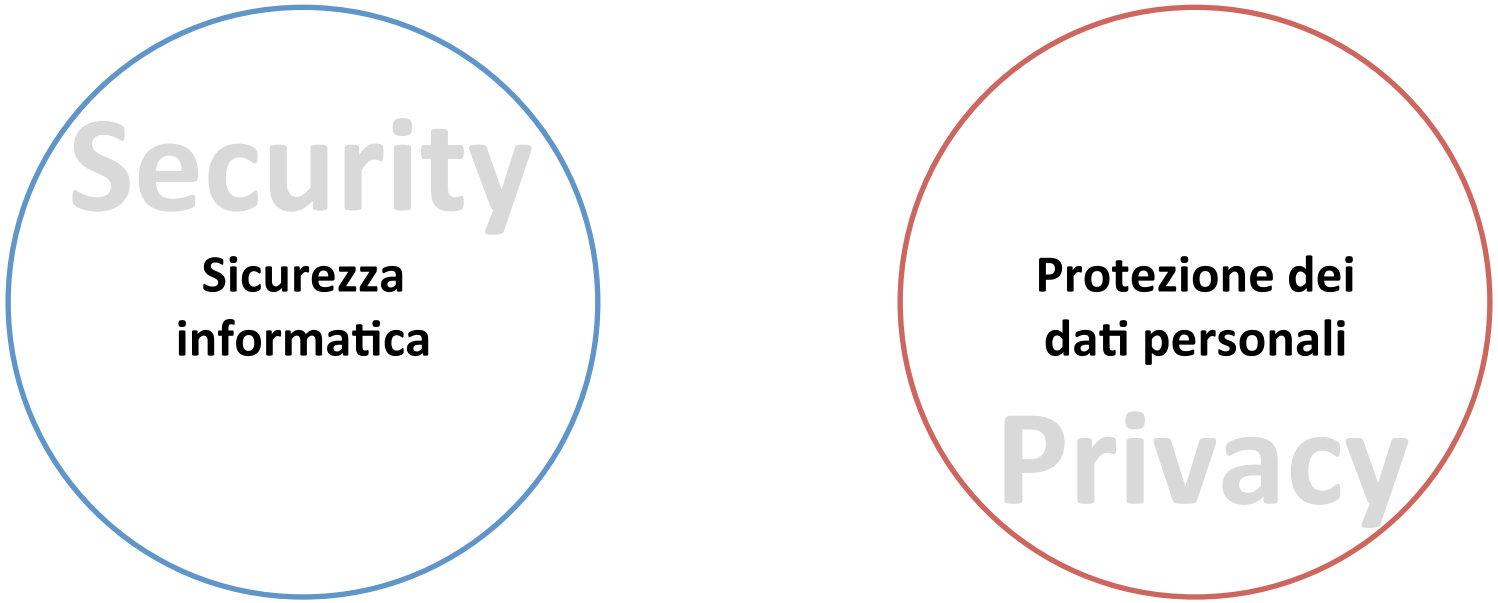


Le leggi si ispirano a **principi comuni** che devono essere poi applicati alle **informazioni**

Le informazioni, in un'economia globale, sono **scambiate intensamente** e con facilità

Rapporto tra Privacy e Security

Il concetto di base su cui è nato il WG5 e su cui poggiano tutti i suoi lavori:



UNINFO

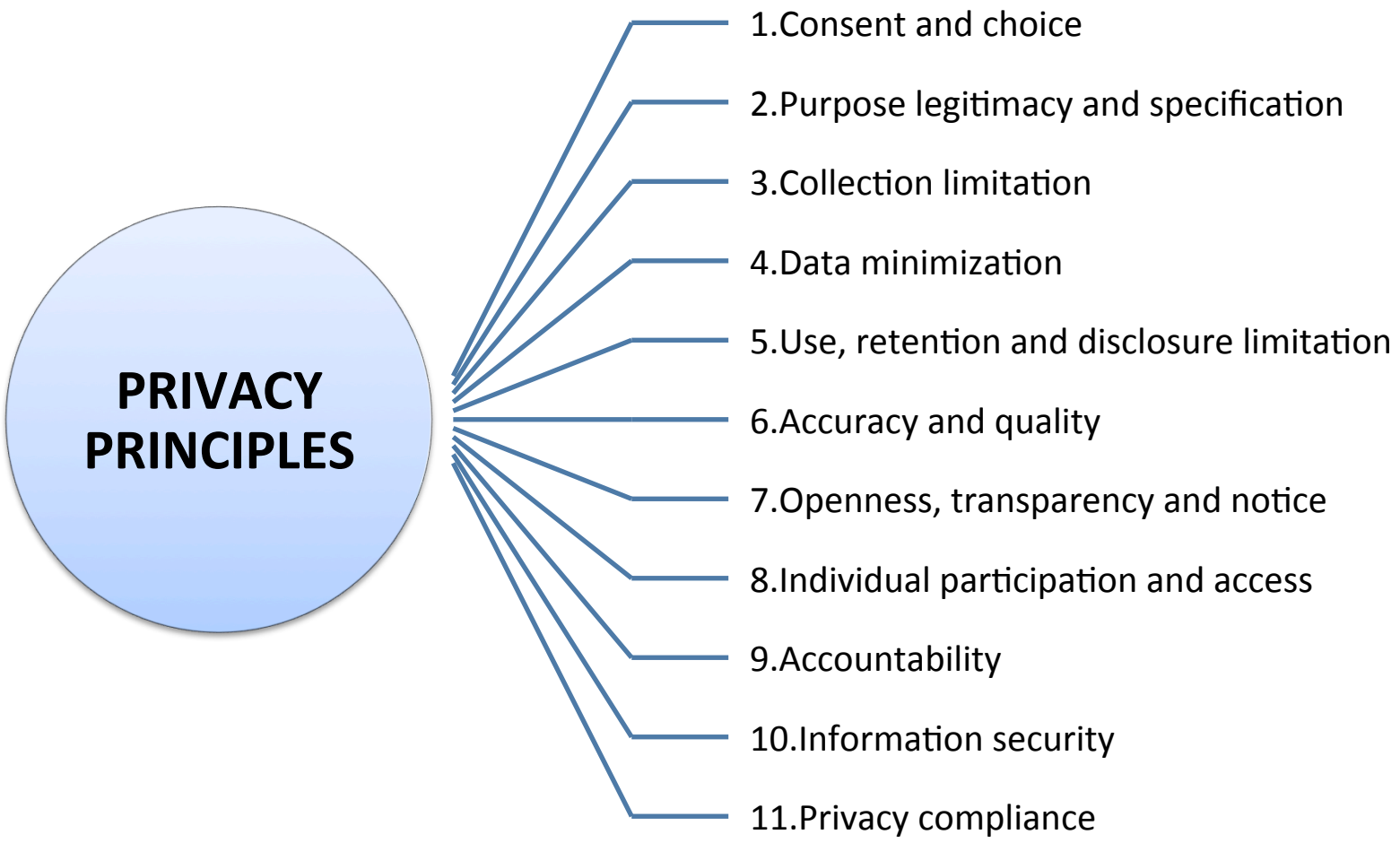
ISO/IEC 29100: Generalità

Framework per la protezione dei dati personali trattati con sistemi informativi

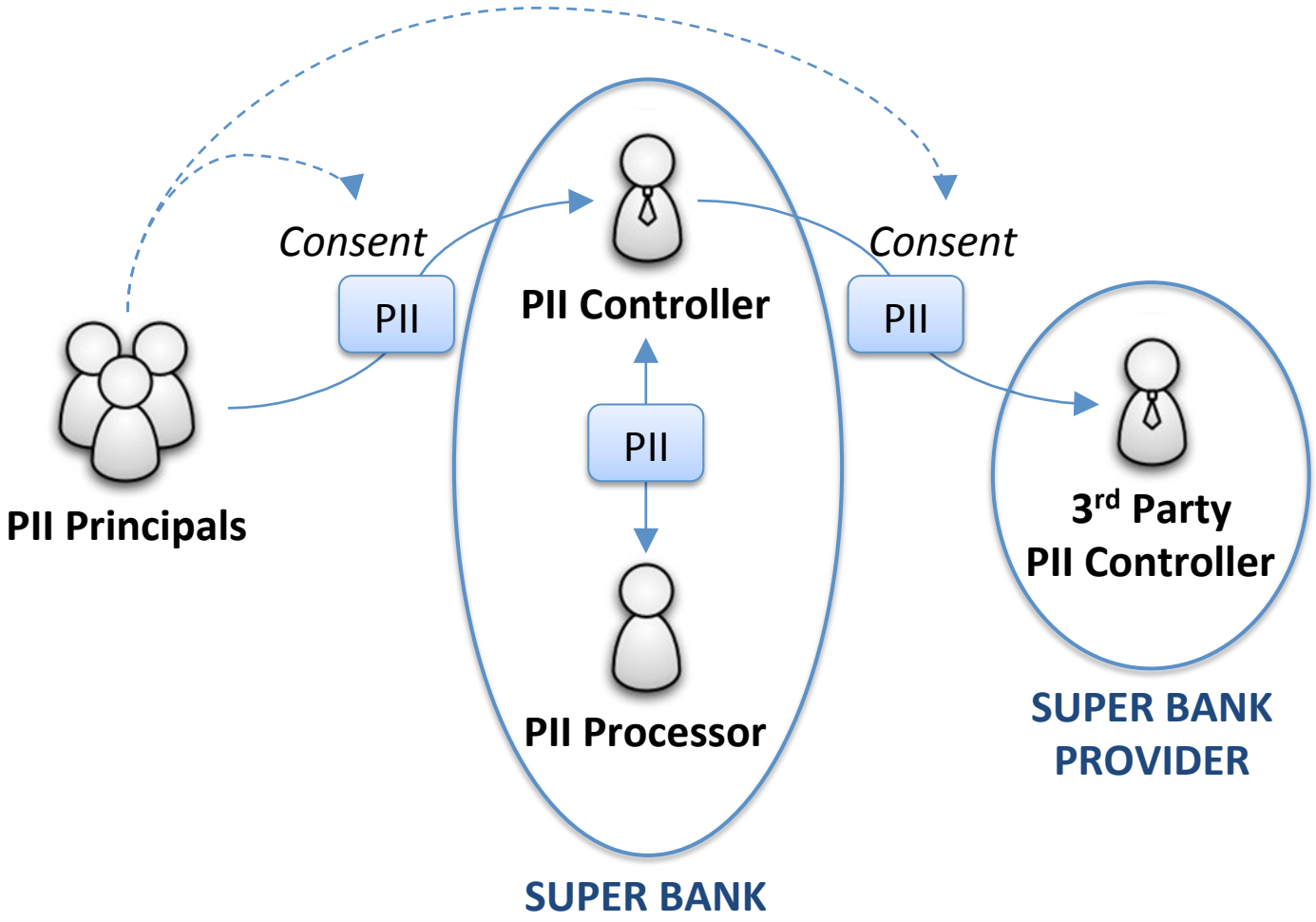
- Definizione di termini (**vocabolario**) condivisi per il trattamento delle PII
- Individuazione di **attori e ruoli** per la gestione dei PII
- Analisi delle **interazioni** tra attori in scenari diversi di trattamento delle PII
- **Classificazione** delle PII
  - Considerazioni su metadati e PII non richieste
  - Tecniche di anonimizzazione o associazione a pseudonimi
- **Gestione dei rischi** relativi alla privacy
- **Misure di sicurezza** per far fronte ai rischi individuati
- **Privacy policy**

Liberamente disponibile in inglese e in attesa di pubblicazione in italiano

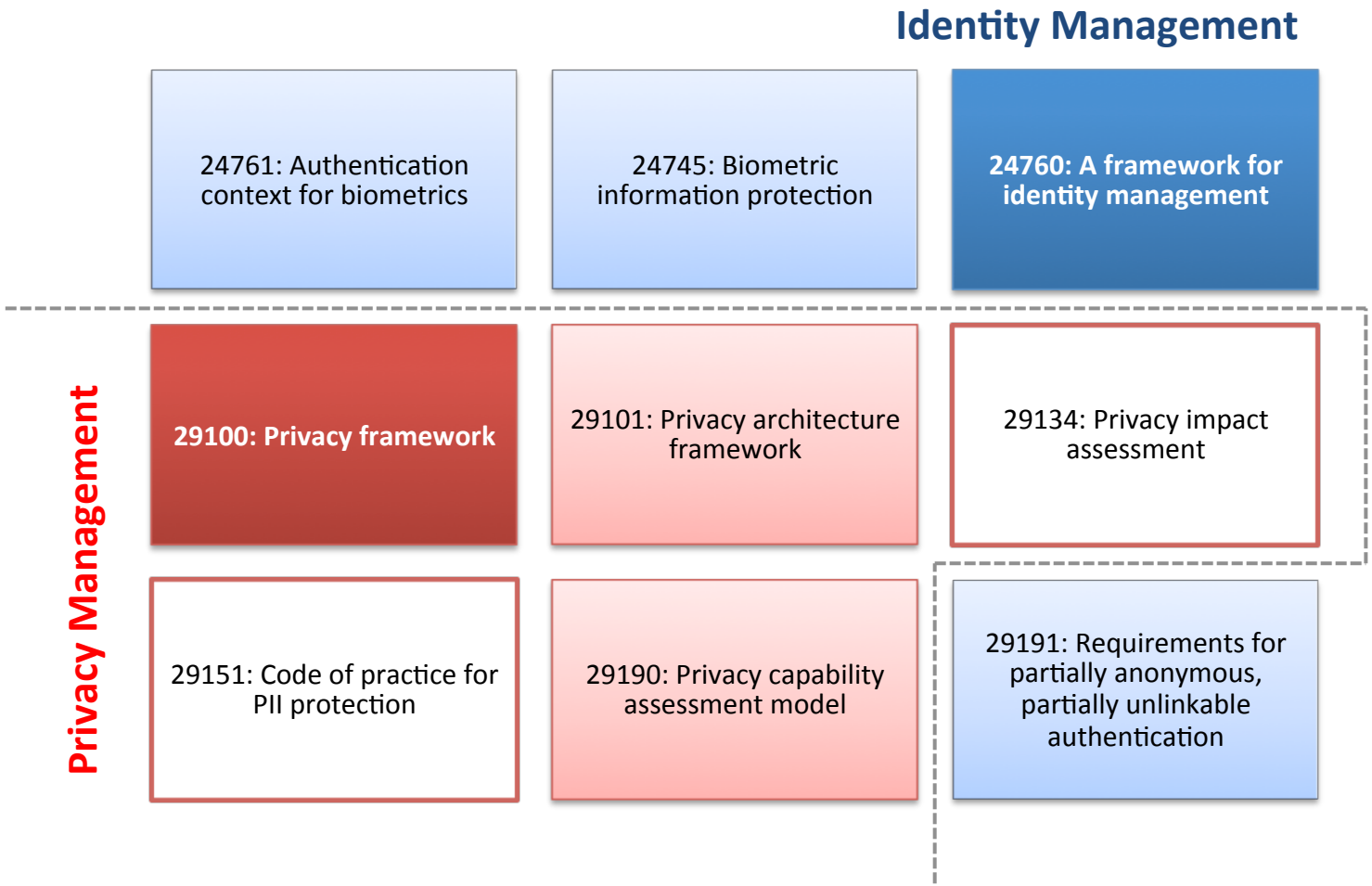
ISO/IEC 29100: Principi



ISO/IEC 29100: Ruoli



Altre norme in lavorazione nel WG5



UNINFO

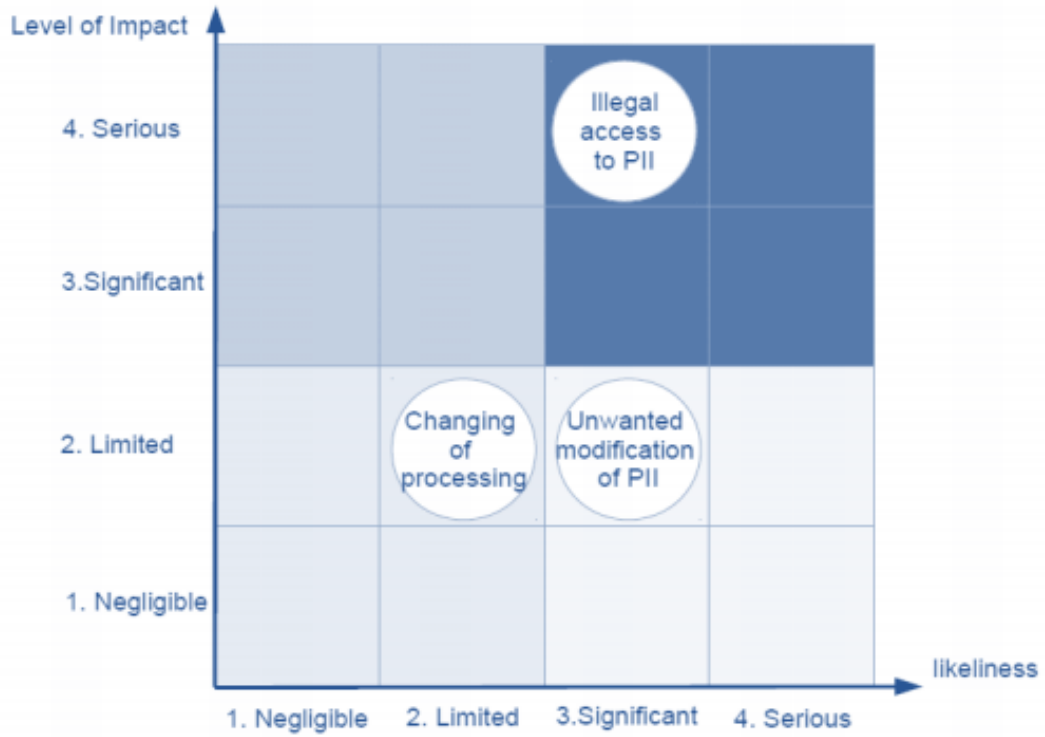
ISO/IEC 29134

Metodologia per condurre un **Privacy Impact Assessment** funzionale a:

- **identificare rischi** relativi alla privacy e responsabilità collegate
- fornire input per la progettazione di sistemi ("**privacy by design**")
- riesaminare l'impatto sulla protezione delle PII di un **sistema nuovo oppure soggetto a modifiche** significative
- **allocare risorse** per il contenimento di impatti sulla privacy
- **fornire informazioni** su ambiti in cui la protezione dei dati personali è un tema chiave
- **fornire evidenza di conformità** dove questa è richiesta
- **fornire evidenza** ai PII principal **delle misure di protezione** presenti sul trattamento delle loro PII

ISO/IEC 29134

ISO/IEC 29134



- Segue un classico approccio di risk management secondo la ISO 31000
- Porta a definire azioni per mitigare il rischio prendendo spunto dal catalogo presente nella ISO/IEC 29151
- Include allegati che propongono tassonomie di minacce e rischi direttamente utilizzabili

I rischi possono essere anche legati a **misure sanzionatorie** legate alla normativa locale

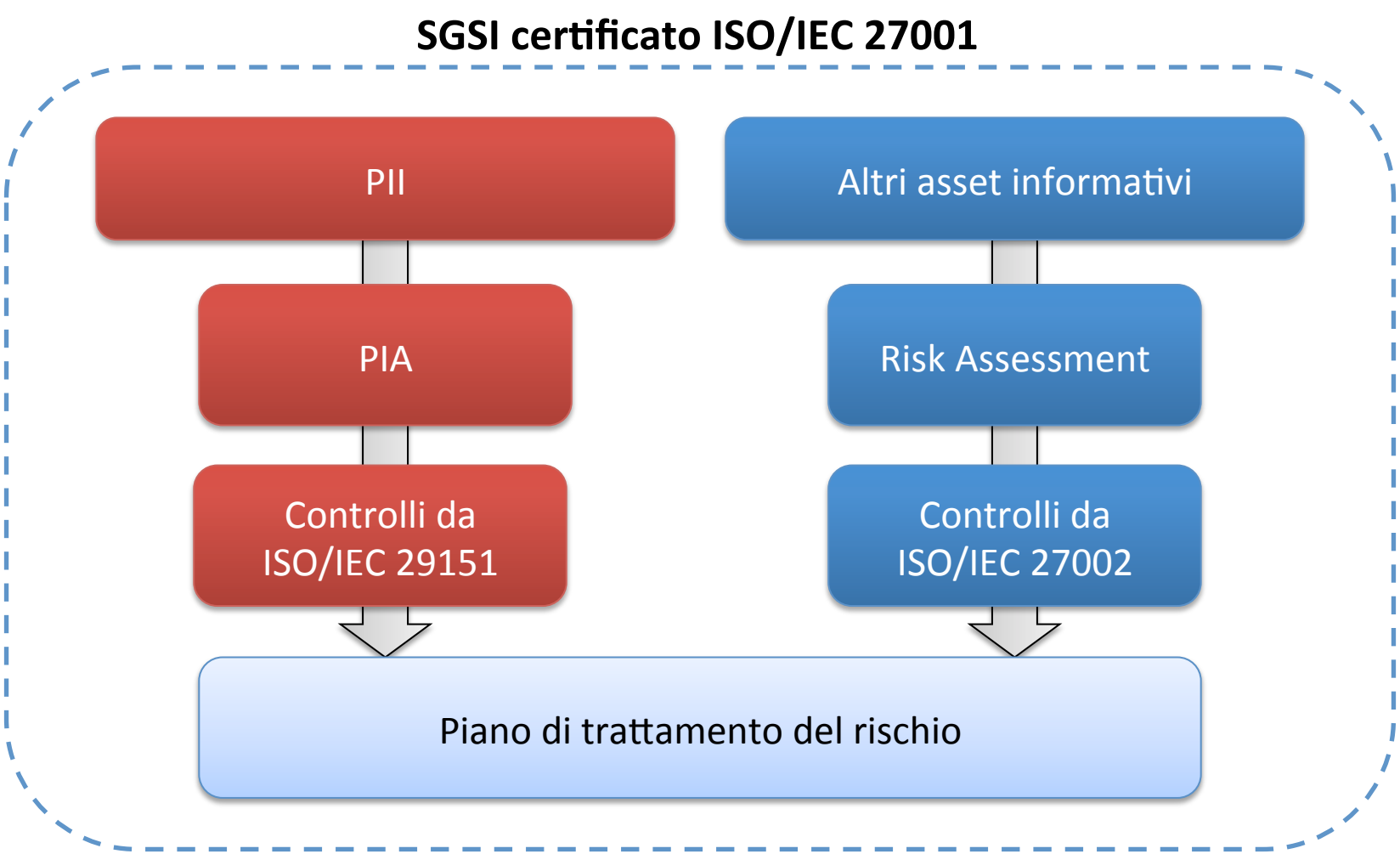
ISO/IEC 29151

Catalogo di **controlli per la protezione dei dati personali** pensato per mitigare i rischi relativi alla privacy (c.d. "privacy risks"). Alcuni esempi:

Policies for the protection of PII	Use, retention and disclosure limitation	Secure erasure of temporary files	PII disclosure notification	Recording of PII disclosures	Disclosure of sub-contracted PII processing
Privacy notice	Dissemination of privacy program information	PII principal access	Redress and participation	Complaint management	Privacy risk assessment
Privacy requirement for contractors and service providers	Privacy monitoring and auditing	PII protection awareness and training	PII protection reporting	Continuous Improvement of PII management systems	Cross border data transfer restrictions in certain jurisdictions

Recepisce completamente i principi della ISO/IEC 29100 ed è calata nel framework della ISO/IEC 27002, risultando compatibile con la ISO/IEC 27001

Scenari di applicazione combinata



Altre attività di SC27 legate alla Privacy

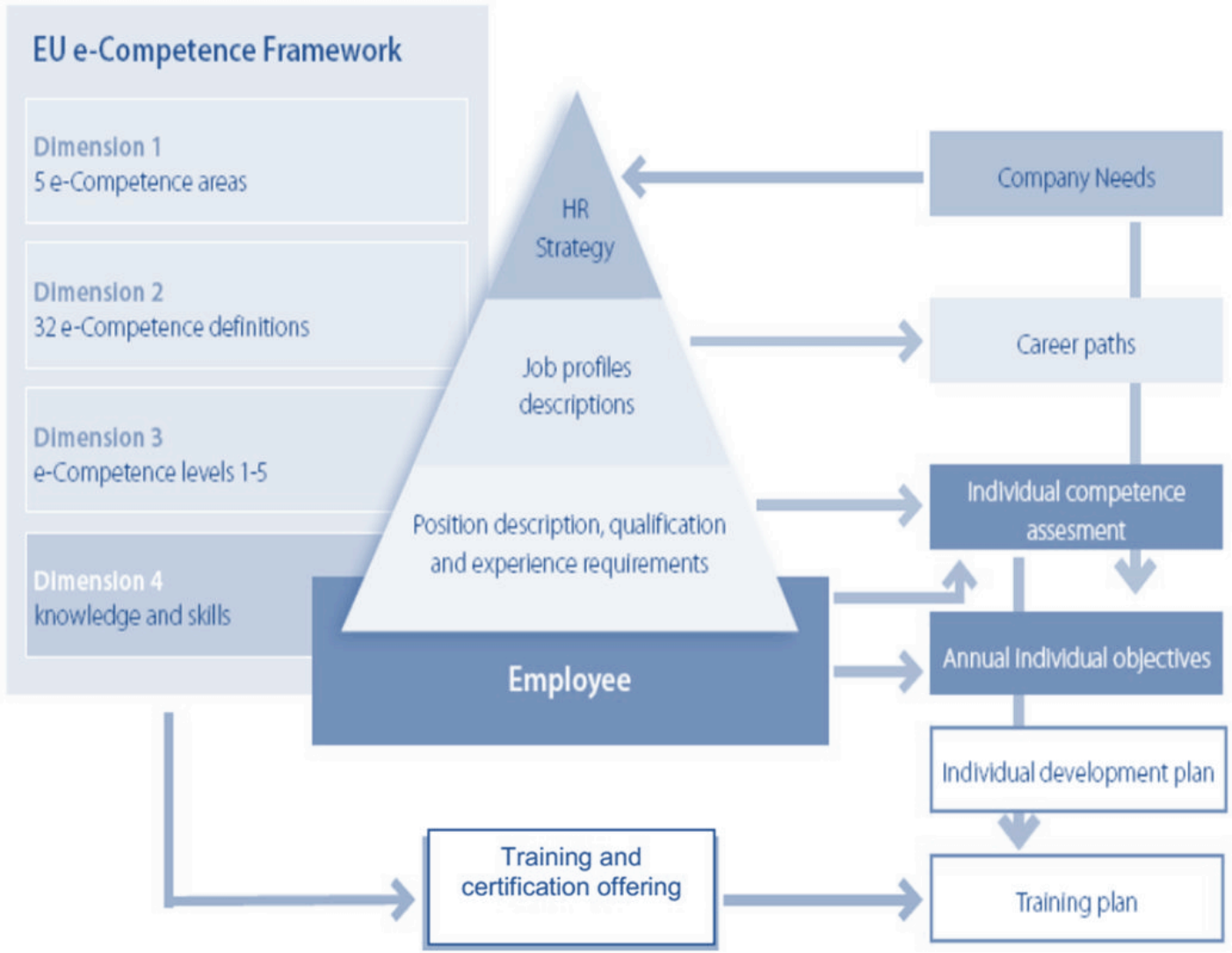
CEN JWG8 costituito a dicembre 2014 su mandato della Commissione per lavorare nell'ambito di "**Privacy management in products and services**" a partire da:

- *"how to address and to manage privacy issues during the design, the development, and the production and service provision processes of security technologies";*
- *"an informative document for the manufacturers and service providers when specifying the privacy management processes with explanations how to realise them";*
- *"adoption as ENs of ISO/IEC 27009 and of ISO/IEC 29134".*

Proposta di realizzazione di uno schema di certificazione volto a riconoscere un "**Privacy Seal**" basato sull'art.39 della proposta di Regolamento.

"**Profili professionali per la data privacy**" basato su e-CF.

Profili professionali: e-CF/UNI 11506



UNINFO

Profili professionali relativi alla privacy

La presente proposta di norma vuole utilizzare gli strumenti messi a disposizione dalla collegata "Metodologia per la costruzione di profili professionali basati sul sistema e-CF" per definire i profili professionali di terza generazione relativi alla gestione della privacy.

Il mercato nazionale è caratterizzato da anni dall'offerta di numerose **proposte di figure professionali di tipo proprietario** legate a questa tematica che, in un'ampia eterogeneità, confondono significativamente l'utente finale, sia questo il privato cittadino che vuole migliorare il proprio profilo professionale o un'organizzazione alla ricerca del professionista adatto a coprire le proprie esigenze.

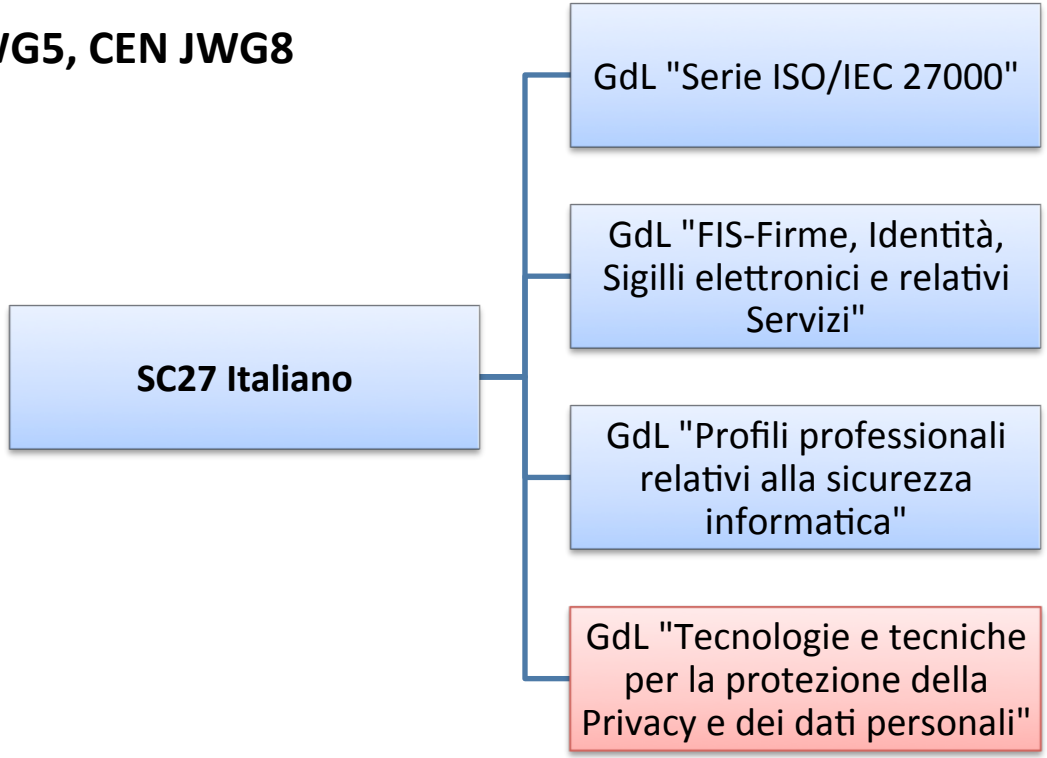
La definizione di **profili condivisi dal mercato** e in grado di armonizzare l'offerta e la domanda in questo settore potrà costituire un valore aggiunto significativo a livello nazionale, permettendo uno sviluppo sinergico da parte dei vari attori e abilitando un miglioramento progressivo delle professionalità legate alla gestione del tema della privacy.

Nuovo GdL UNINFO in SC27

CAMPO DI ATTIVITÀ

Sviluppo e manutenzione di norme nazionali e internazionali relative agli aspetti tecnologici e alle tecniche in materia di protezione della Privacy e dei dati personali

MIRROR SC27 WG5, CEN JWG8



Contatti e ringraziamenti

UNINFO
http://www.uninfo.it/
uninfo@uninfo.it
Corso Trento 13 - 10129 Torino
Tel. +39 011501027 - Fax +39 011501837

Relatore della presentazione:

Fabio GUASCONI – Presidente SC27 UNINFO
fabio.guasconi@bl4ckswan.com