Profili di garanzia delle identità digitali della Federazione IDEM

Davide Vaghetti – davide.vaghetti@garr.it

GARR

Agenda

- Identity Assurance Framework e RAF
- Profili di garanzia IDEM
- Requisiti
- Casi d’uso
- Segnalazione, richiesta, asserzione
- Ambito, Conformità e Verifica

Identity Assurance Framework

REFEDS

REFEDS Assurance Framework 1.0

ITU

ITU-T X.1254 (ISO/IEC 29115:2019)

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

Special Publication 800-63-3

European Commission

REGOLAMENTO DI ESECUZIONE (UE) 2015/1502 DELLA COMMISSIONE

SPID
CIE

kantara INITIATIVE

Kantara Initiative Identity Assurance Framework: Service Assessment Criteria

REFEDS Assurance Framework
Casi d'uso

LIFE SCIENCE RI

- Risorse ELIXIR
- Risorse BBMRI

neic PUHURI

- LUMI
- FENIX

NIH National Institutes of Health
Turning Discovery Into Health

- Grant Programs
- Datasets
- Research collaborations

REFEDS Assurance Framework 1.0

Multidimensionale

Identificatori, Verifica identità, Qualità attributi + Autenticazione

Semplice

Più complicate sono le specifiche, minore sarà l'adozione

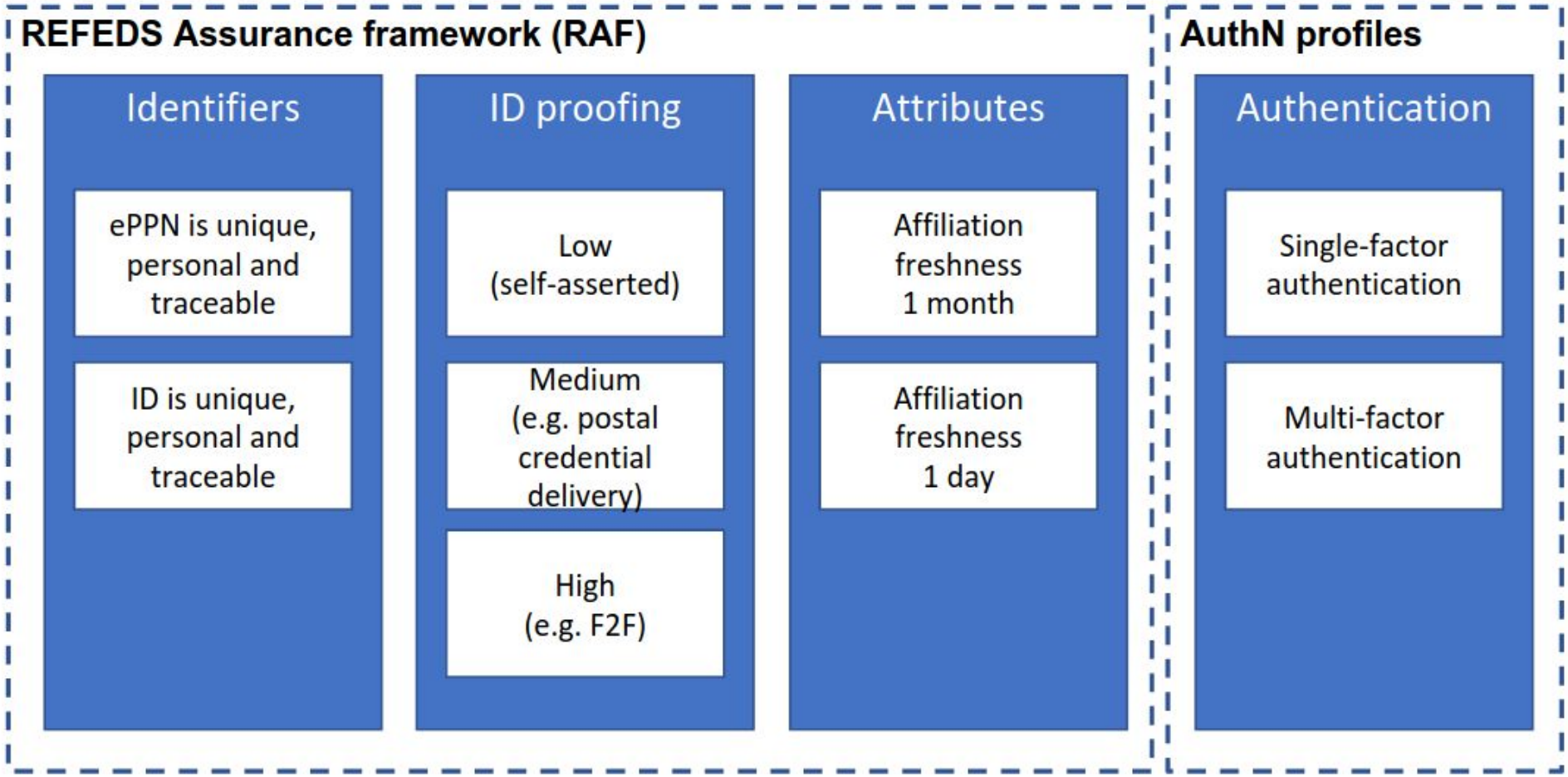
Non reinventa la ruota (RAF 2.0)

Riferimento a ITU X.1254, eIDAS LoA, NIST SP 800-63-3, Kantara Identity Assurance Framework, IGTF Levels of Authentication Assurance

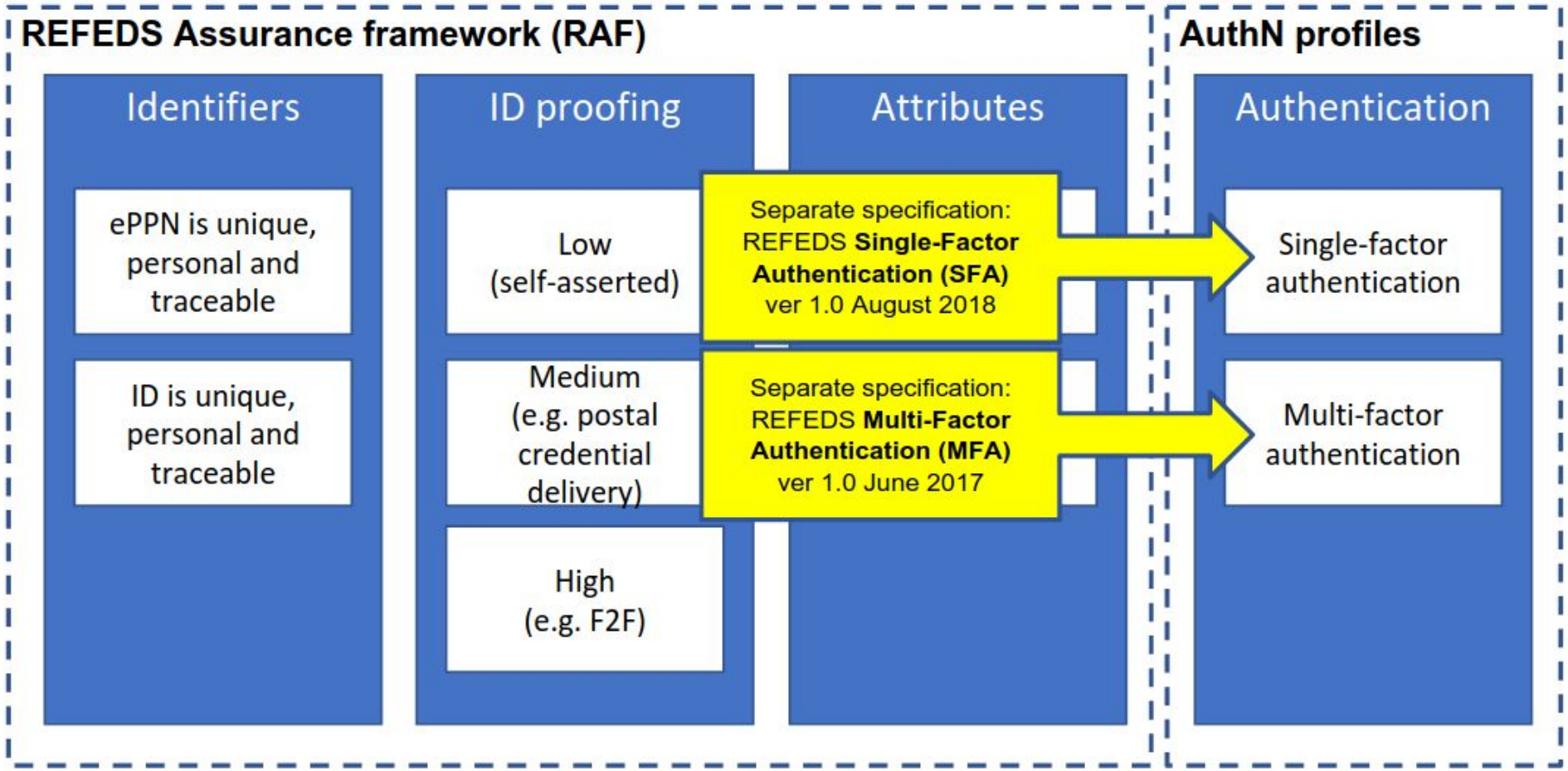
Trasversale

Federazioni di identità della ricerca e dell'educazione, Infrastrutture e collaborazioni di ricerca, Servizi e Risorse commerciali

The big picture of assurance in REFEDS



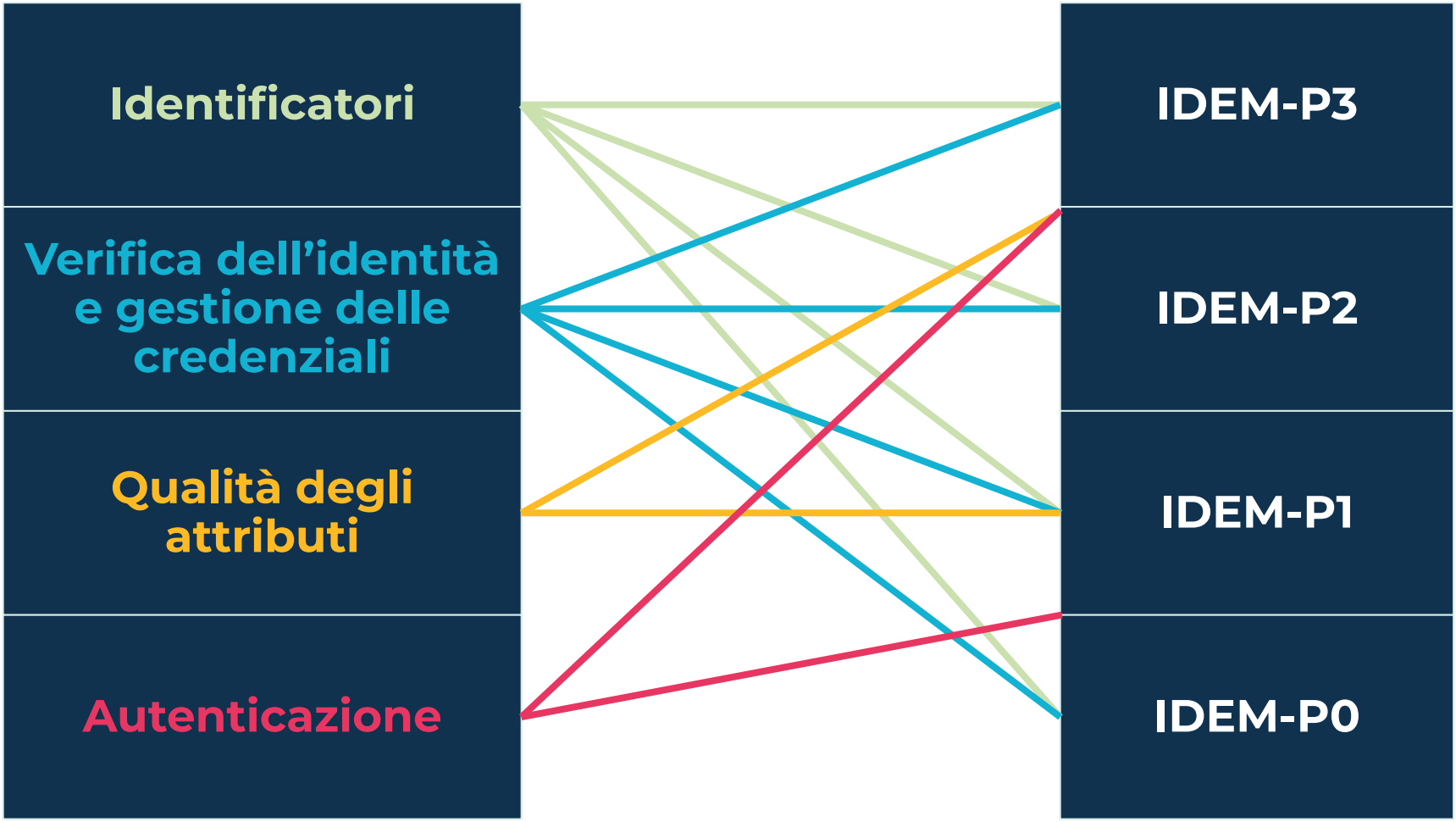
Split of responsibility between REFEDS specs



Profili di garanzia IDEM

1. Accesso ai servizi REFEDS Assurance Framework
2. Rispetto norme europee e standard internazionali
3. Diffusione standard di sicurezza e autenticazione a più fattori (MFA)

Profili di garanzia IDEM



Requisiti: Identificatori

- Identificatori di protocollo (SAML 2.0/OIDC 1.0)
- Persona fisica
- Contattabile
- No riassegnazione

Verifica dell'identità e gestione delle credenziali

- Registrazione e accreditamento
- Controllo e verifica dell'identità
- Emissione, consegna e attivazione
- Sospensione, revoca e riattivazione
- Rinnovo e sostituzione

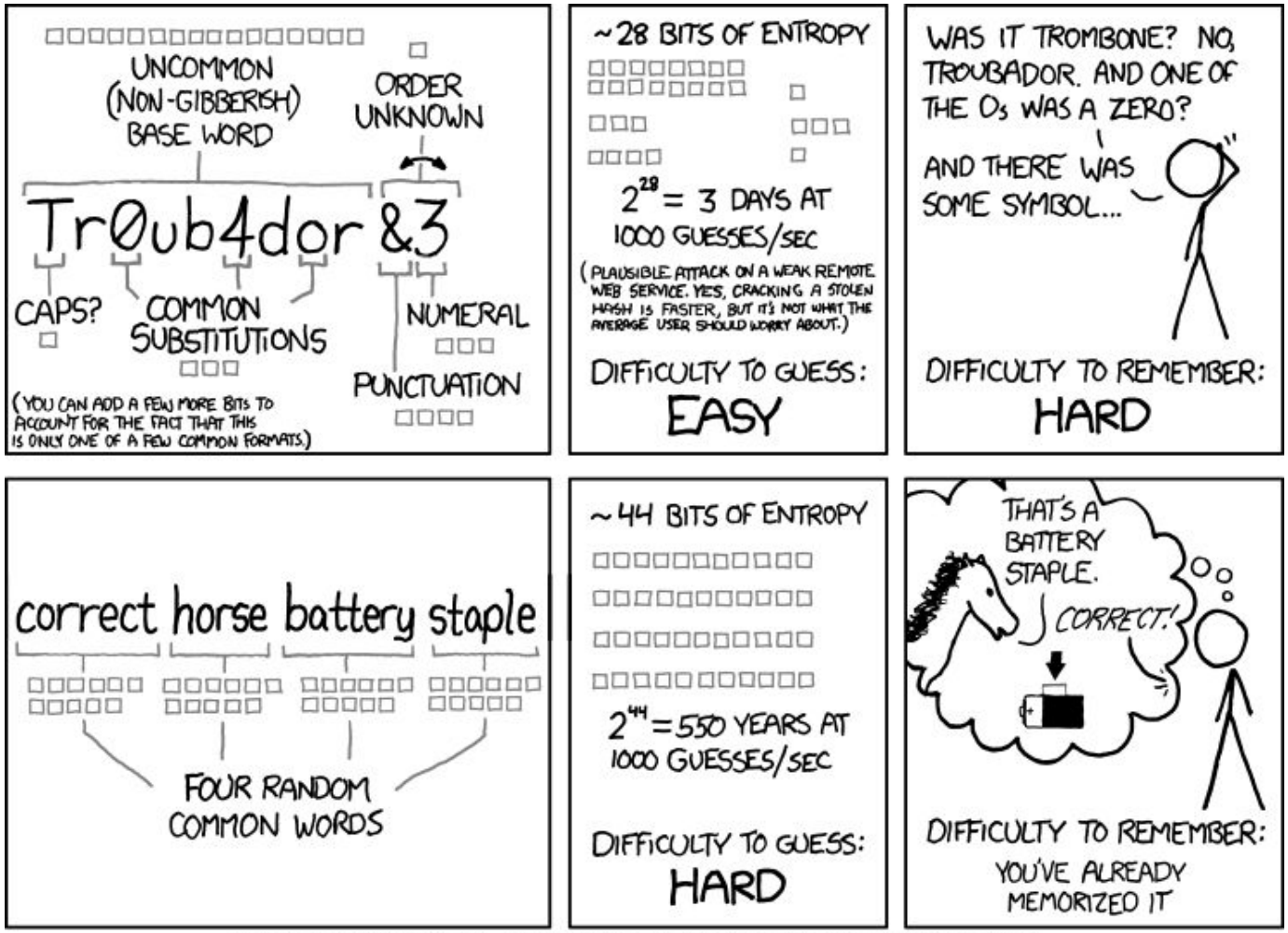
Qualità degli attributi

- Affiliazione: student, staff, member
- Aggiornamento entro 1 mese
- Aggiornamento entro 1 giorno

Autenticazione a singolo fattore

Tipo di autenticazione	Specifiche base	Lunghezza minima
Segreto memorizzato	>= 52 caratteri	12 caratteri
	>= 72 caratteri	8 caratteri
OTP (segreti generati e usati una sola volta)	10-51 caratteri	6 caratteri
	>= 52 caratteri	4 caratteri
Segreto ad uso singolo	10-51 caratteri	10 caratteri
	>= 52 caratteri	6 caratteri
Chiavi crittografiche	RSA	2048 bit
	ECDSA	256 bit

Password strength



THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

https://xkcd.com/936

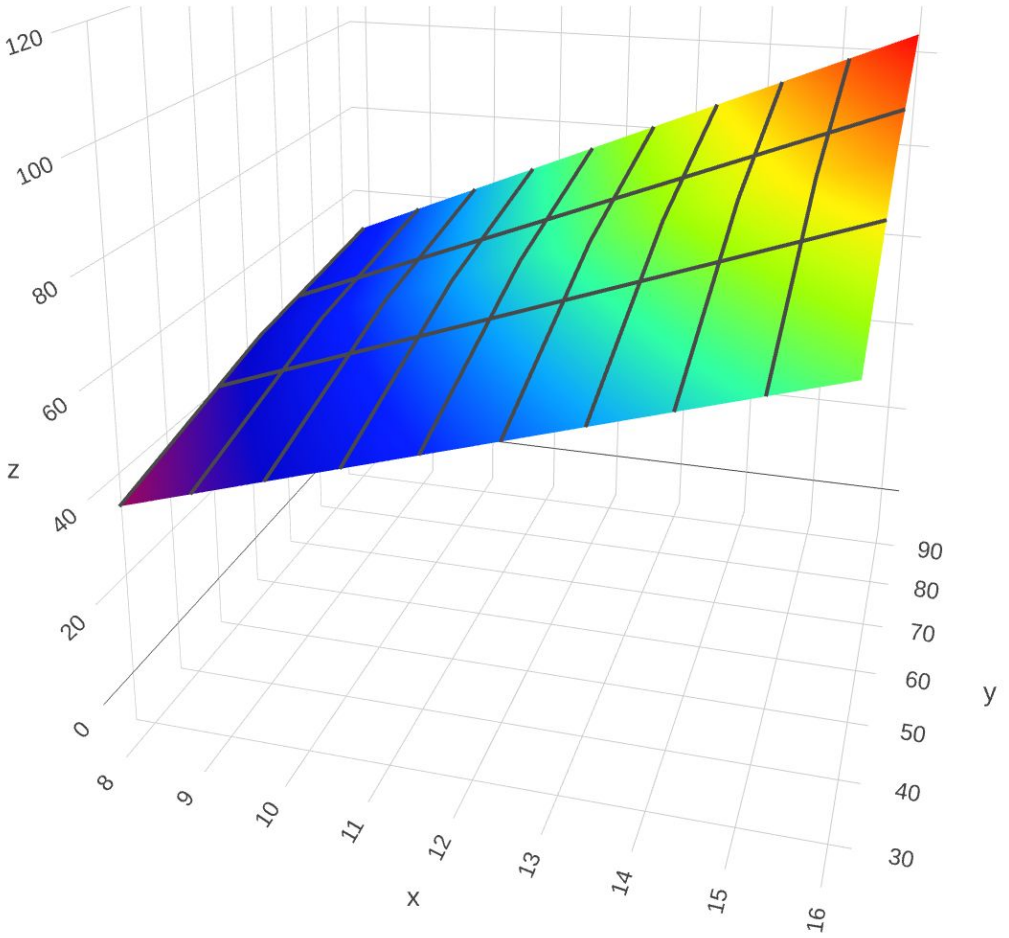
$E=L*\log_2(B)$

x=lunghezza password

y=base caratteri

z=password entropy

x	z, y=26	z, y=62	z, y=92
8	41.1	47.6	52.1
10	47.0	59.5	65.2
12	56.4	71.4	78.2
14	65.8	83.3	26
16	75.2	95.2	104.3



Autenticazione a più fattori

- Combinazione più fattori o dispositivi multifattore
- Fattori di tipo diverso
- Fattori indipendenti
- **Eccezione**, attivazione ulteriore fattore:
  - misure ulteriori, ad es. processo supervisionato
  - **sempre** notifica utente

IDEM-P0

Caso d'uso	Test di ingresso / autovalutazione per l'iscrizione all'università, iscrizione a portali web tramite auto-registrazione.
Verifica identità	Identificazione tramite verifica del contatto (email, numero di telefono).
Autenticazione	Singolo fattore

IDEM-P1

Caso d'uso	Immatricolazione di uno studente.
Verifica identità	Identificazione tramite **esibizione di un documento di identità apparentemente autentico** o identificazione tramite altre credenziali, ad esempio SPID-L1.
Affiliazione	Aggiornata almeno entro un mese.
Autenticazione	Singolo fattore.

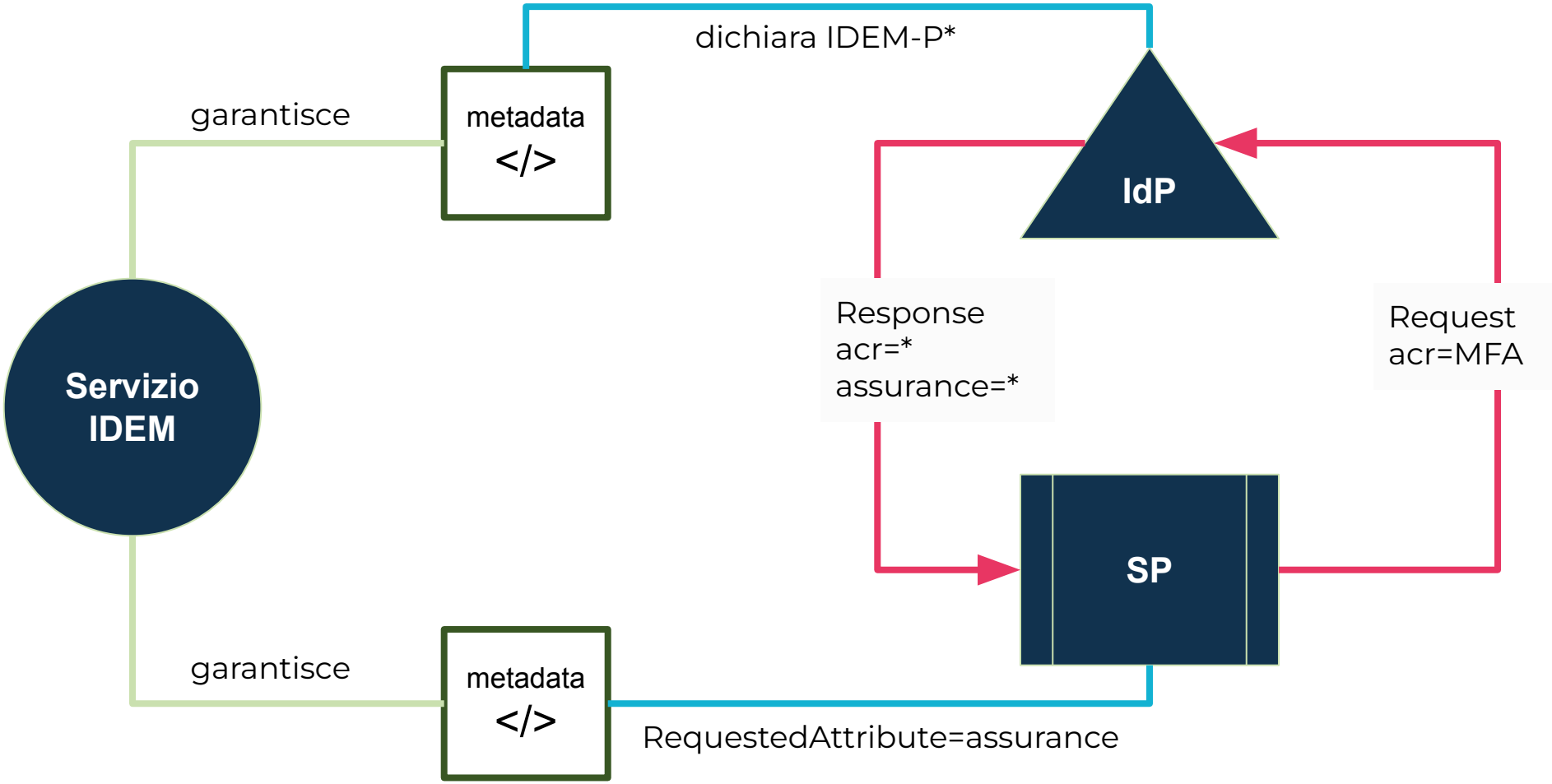
IDEM-P2

Caso d'uso	Registrazione di un dipendente.
Verifica identità	Identificazione tramite **esibizione di un documento di identità e ulteriori verifiche tramite altri documenti**, o identificazione tramite altre credenziali, ad esempio SPID-L2
Affiliazione	Aggiornata almeno entro un giorno.
Autenticazione	Più fattori.

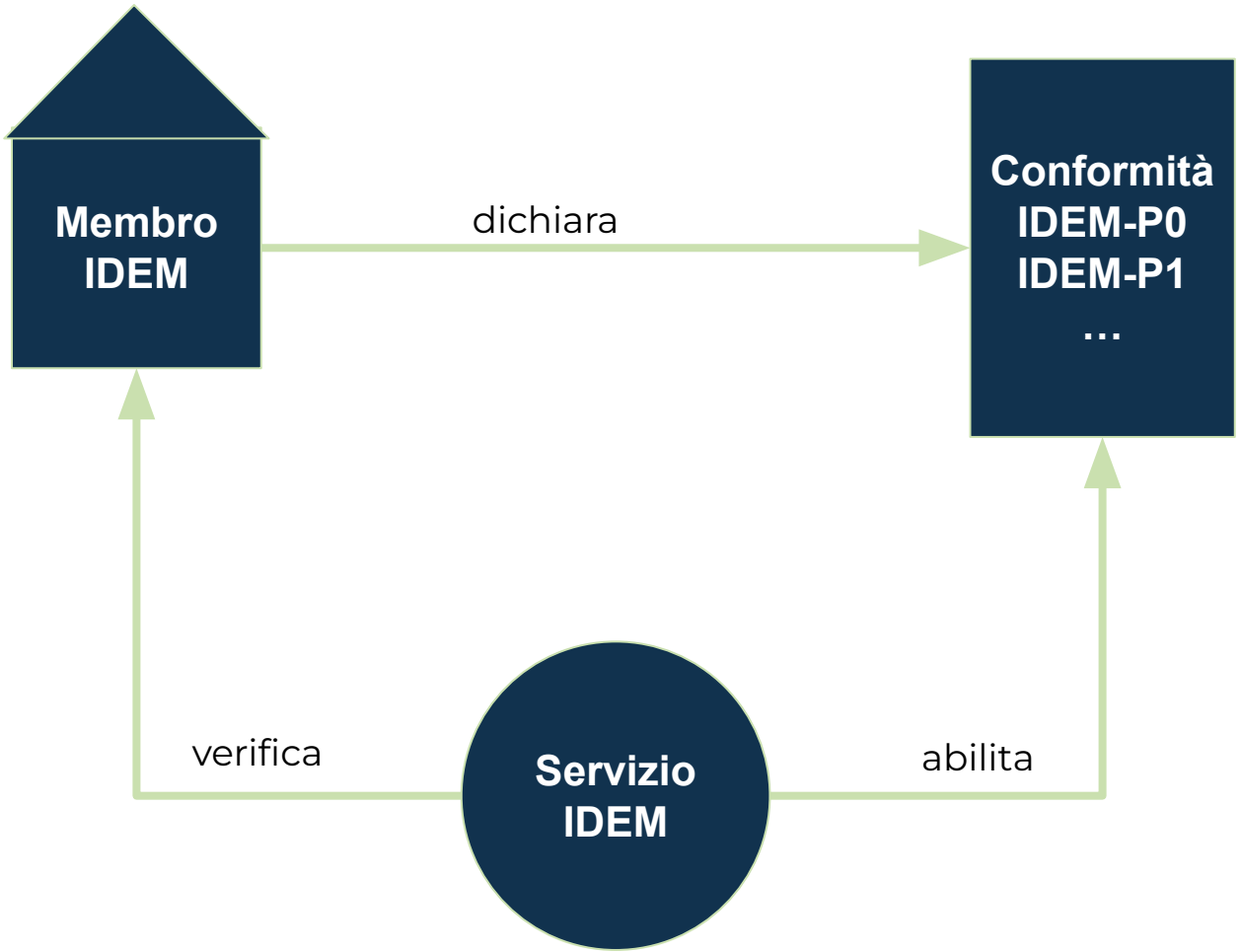
IDEM-P3

Caso d'uso	Assegnazione di account per accesso a dati particolari e/o servizi altamente critici.
Verifica identità	Identificazione tramite altre credenziali come CIE o superiori.
Affiliazione	Aggiornata almeno entro un giorno.
Autenticazione	Più fattori.

Segnalazione, richiesta, asserzione



Ambito, Conformità e Verifica



Grazie al gruppo di lavoro Identity Assurance!

Arianna Arona, Francesco Zanolin, Stefano Colagreco, Simone Lanzarini, Silvio Scipioni, Andrea Ranaldi, Enrico Maria Vincenzo Fasanelli, Antonella Monducci, Loredana Martuscello, Davide Vaghetti

Grazie per l’attenzione

https://wiki.idem.garr.it/wiki/ConsultazioneProfiliDiGaranziaIDEM