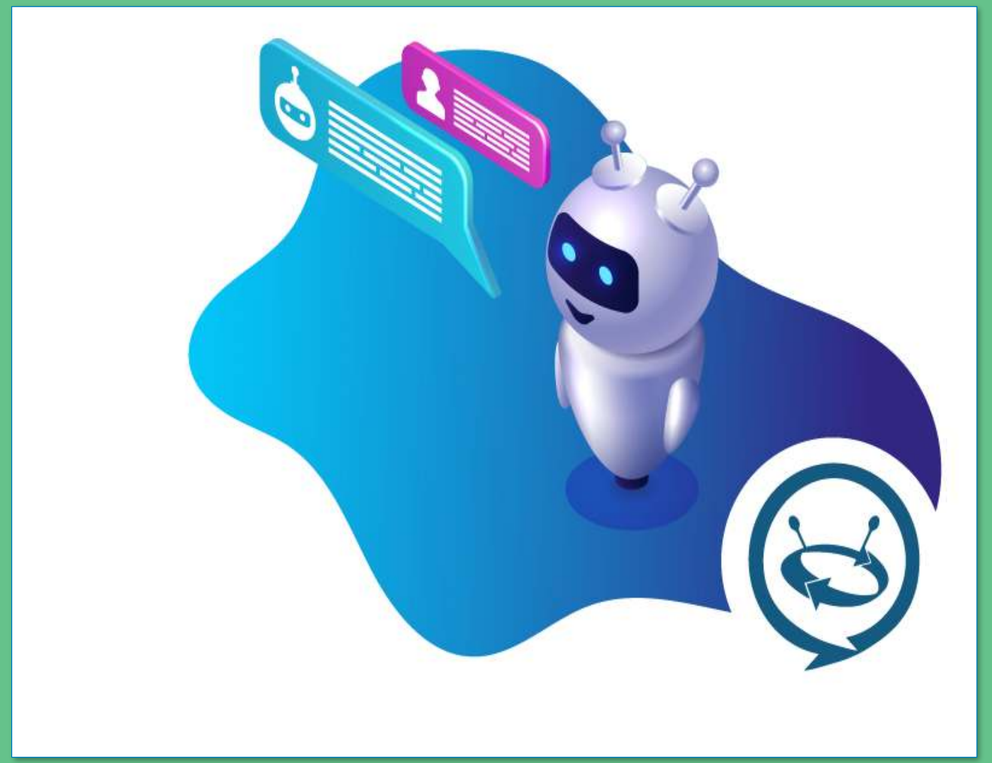
L'Identità Digitale: ieri, oggi e domani



a/simmetrie

28 Luglio 2022

Vincenzo Di Nicola

Responsabile per l'Innovazione Tecnologica e la Trasformazione Digitale - INPS

@vincenzo @vincenzo vincenzo@inps.it

Identità Digitale.
A cosa serve?

- Nel mondo online, a provare che io sono chi dico di essere
- Accedere così a servizi digitali a cui sono abilitato

Ieri e oggi: esempio militare

BOLLETTINO DI GUERRA
del
Comando Supremo

4 novembre 1918.

La guerra contro l'Austria-Ungheria che, sotto l'alta guida di S. M. il Re, Duce Supremo l'Esercito Italiano, inferiore per numero e per mezzi, iniziò il 24 maggio 1915 e con fede incrollabile e tenace valore condusse ininterrotta ed asprissima per 41 mesi, è vinta.

La gigantesca battaglia, ingaggiata il 24 dello scorso ottobre, ed alla quale prendevano parte 51 divisioni italiane, 3 britanniche, 2 francesi, una czeco-slovacca, ed un reggimento americano, contro 73 divisioni austro-ungariche, è finita.

La fulminea, arditissima avanzata del 29° Corpo d'Armata su Trento, sbarrando le vie della ritirata alle armate nemiche del Trentino, travolte ad occidente dalle truppe della 7ª Armata e ad oriente da quelle della prima, sesta e quarta, ha determinato ieri lo sfacelo totale del fronte avversario.

Dal Brenta al Torre, l'irresistibile slancio della dodicesima, dell'ottava, della decima armata, e delle Divisioni di cavalleria ricaccia sempre più indietro il nemico fuggente.

Nella pianura S. A. R. il Duca d'Aosta avanza rapidamente alla testa della sua invitta terza Armata, anelante di ritornare sulle posizioni che essa aveva già vittoriosamente conquistate.

L'esercito austro-ungarico è annientato. Esso ha subito perdite gravissime nell'accanita resistenza dei primi giorni di lotta, e nell'inseguimento ha perduto quantità ingentissime di materiale di ogni sorta e pressochè per intero i suoi magazzini e depositi; ha lasciato finora nelle nostre mani circa 300 mila prigionieri con interi Stati Maggiori e non meno di 5000 cannoni.

I resti di quello che fu uno dei più potenti eserciti del mondo risalgono in disordine e senza speranza le valli che avevano disceso con orgogliosa sicurezza.

DIAZ.

"I resti di quello che fu uno dei più potenti eserciti del mondo risalgono in disordine e senza speranza le valli che avevano disceso con orgogliosa sicurezza"

Identità Digitale di Armando Diaz

Firmato Diaz

Nota storica: da Giulio Cesare alla NSA americana, i bisogni militari hanno dato enorme impulso all'evoluzione della crittografia

Crittografia asimmetrica

BOLLETTINO DI GUERRA
del
Comando Supremo

4 novembre 1918.

La guerra contro l'Austria-Ungheria che, sotto l'alta guida di S. M. il Re, Duce Supremo l'Esercito Italiano, inferiore per numero e per mezzi, iniziò il 24 maggio 1915 e con fede incrollabile e tenace valore condusse ininterrotta ed asprissima per 41 mesi, è vinta.

La gigantesca battaglia, ingaggiata il 24 dello scorso ottobre, ed alla quale prendevano parte 51 divisioni italiane, 3 britanniche, 2 francesi, una czeco-slovacca, ed un reggimento americano, contro 73 divisioni austro-ungariche, è finita.

La fulminea, arditissima avanzata del 29° Corpo d'Armata su Trento, sbarrando le vie della ritirata alle armate nemiche del Trentino, travolte ad occidente dalle truppe della 7ª Armata e ad oriente da quelle della prima, sesta e quarta, ha determinato ieri lo sfacelo totale del fronte avversario.

Dal Brenta al Torre, l'irresistibile slancio della dodicesima, dell'ottava, della decima armata, e delle Divisioni di cavalleria ricaccia sempre più indietro il nemico fuggente.

Nella pianura S. A. R. il Duca d'Aosta avanza rapidamente alla testa della sua invitta terza Armata, anelante di ritornare sulle posizioni che essa aveva già vittoriosamente conquistate.

L'esercito austro-ungarico è annientato. Esso ha subito perdite gravissime nell'accanita resistenza dei primi giorni di lotta, e nell'inseguimento ha perduto quantità ingentissime di materiale di ogni sorta e pressochè per intero i suoi magazzini e depositi; ha lasciato finora nelle nostre mani circa **300** mila prigionieri con interi Stati Maggiori e non meno di **5000** cannoni.

I resti di quello che fu uno dei più potenti eserciti del mondo risalgono in disordine e senza speranza le valli che avevano disceso con orgogliosa sicurezza.

DIAZ.

“I resti di quello che fu uno dei più potenti eserciti del mondo risalgono in disordine e senza speranza le valli che avevano disceso con orgogliosa sicurezza”

```
1 -----BEGIN PGP PRIVATE KEY BLOCK---|--
2
3 lQWGBGLieu0BDADNDVqAEDCXzncL9QyurEzhlyTDdOIZt9dk46CKdT4B+xAPETiE
4 S+tSNBqhPCjmy5eikFa6nZv+ik2aNOVfPiZPLLS5DCQJnrtKT/6lpB9zVFRu+Ume
5 Mg2GauXhEUeqox2pS6VTTF1B05+wjU+AldSu/Im+3SSERZrjmSOoHIPBSrJWibxS
6 EppyG8XA0t08+SSUl4MDEZQr8ENqIsvgZjujyGEHhd16rpkAh8Go4Oof9wv6LfbK
7 7OqFpQsM66Rv/wRDzjBvFph1+tiZbOcJUaowkfXXNU0rbCcT25KwBCLD60/plzI2
8 olLcBuNXwfVIkvq3dFcmT49CMczIHT/RFRSqCvifdcF6Id//ukrAuGEHxJlsijbg
9 7u8AE8TXVQq2Jkp20/dUboEBvk6NIZ/TiQM8CfaR+yXQk7niPk5DC2Q3u8GCosit
10 DeNw6oCBySCR1B7DKC2Spl+KVlRA4ui8fB6hAnUa7UXT6JewqppwzlNImcomrKkT
11 X0Ys7AsUlIENPY8AEQEAAf4HAwLKlF4KkHFxWv/h4ePk1+LXNMUZG7mgZfNxc0QI
12 mTsl76q0jx8NF3n0UxfXuFm3zoYxRl6ZcgjgxMAmb5aladu2MGlKLKydLmG3ZvBo
13 Tt6GR+WhdtD1hOSE4dvCIJAK+prUTXbzWDDO1M4QDHqwU9OdqwGoK5gdIdFfqJwK
14 FxPey/ULcNrN53u2IwlfdJpir7n9GSZIIWBn/a1RbRYFzoHtRD4pwZ4+WKrlO4aX
15 Oi5AMlRhCuuPTO2hhoeUJsdmTRF4Uy4tfoxoQbguWbAyNRrUpsIymeNSPz8+avx4
16 PpfJAYE2lR/J9UjUTGCjjNVHIFYmztB8CfWoZ5CxdULzPIF3R/RK+kUnWMHUy6tL
17 rF0byLeWhnsqRhRESFHGJscx3ysPTCa9LVD14K4EB2M8KXL/LP2UI4Us/lCm1gB1
18 ormdjj07yTt+kY1oS0jP/YwQE9NAPC0Ey4ObIA83YCI4gEw+A8o3ELnBAu8TrcFM
19 0mV2ZKhnq2Dh0gmvAREsVzBrc1kxEDFxL+tHTRtRq0Rvgw/wcwdI8GgpvBhi9+8R
20 XSGyprC5buIWTq277V/YoeI3uORjJzt36Dg3sKB5fTnXSsilgfMflzSLK4R1VC+q
21
22 [...]
23
24 pX7bH6Hlh0eIcRGaClFQTYrPxXzWl6BoULP7QNg1Ha+41hNI2Iiq+S0WRchwk+YI
25 5E/9RqYGSyZtHFQADxYDD/Hoa4kOdzhToZ8ZE5BsC7mMVCj74T2A56trJDy/38k0
26 vIgFEwMJ71d8ti40UFb0R6o12bJ5QKfcFcQkMGw4Uw+ghxyBDZ6tT05+KPbEQEv+
27 KlOwFfTCxzD/BXt4UJiEp+AWtqoRnEeUTq0sMUfzWIxissswAJ0mPtUHozCP9y05a
28 jyA0TnKICPRUydU2eLw5CUxFTWfY+qYE2drOFKvkGqQ6zJd0OlJrBgkV2NX1QVCu
29 zbzQRolwZl1TYLgykfL7FS2476BArArBMXCTQjRlZzSbjL8no4bMXRa9Jy2LXvgZ
30 LD+CpfbkxW+SVGXh87dajFjQXr019F8WTkMgF2ObsF70L6
31 /9N2aDLVQQotLX1DGwoSU5m1tDK3qQHeJ0LzNXU/QE3
32 ZVSu97O+/cIfBPirJRcl/Jy4k/mFCszIczFa6N
33 wERkmQL7fxkSZIdqTWuF0huSEHBHrdSIPbt+7
34 Ho7JQyFtL9zm9hYFqAz/DvcDaoT/yUUsC58
35 gblkfeBaL0w4brzr5sooQCCJ6rYSY2Aj1
36 /lspWgRVtRMMbjzGpBUlAwCLTislM59k
37 WwfPgDOwobwyg5pogE/KB6zQ+/9fDSR
38 kAWAcwXnLkWKdCcankpgwJUxakJQut
39 WR5r6bxotLTBTwUCYuJ67QIbDAUJA8
40 8mJtW34GVl7YOt47XfoBB218WNM/D
41 6rjX+898jXFrYEMoHrlkbtMoMrldJE
42 a4PqYbKQY042cmagJVcMJW717krNPB
43 yHzzvlw2/vduLtO0IGsiJI+qDsSsZCSh
44 61RfGohftHdZ/yD9aiTX/xJQrYnBSD4j5w
45 WxbUCkVQy26yrhP2ApQcQOQM5txSCl22fNr/9JFsP+t
46 gKP0turrj2ciAd39njEwXGftg4VjpDQwkBX+1CY+LK
47 EvE+BM93HHIlNugGDyOOjd5USNgoQUC2bFlr+7HsL+D
48 =nX2h
49 -----END PGP PRIVATE KEY BLOCK-----
```

Chiave **Privata** di Armando Diaz

=

=

```
1 -----BEGIN PGP SIGNED MESSAGE-----
2 Hash: SHA512
3
4 I resti di quello che fu uno dei più potenti eserciti del mondo risalgono
  in disordine e senza speranza le valli che avevano disceso con orgogliosa
  sicurezza.
5 -----BEGIN PGP SIGNATURE-----
6
7 lQGzBAEBCgAdFiEEZuwm4z70r1kVVFkea+m8aLS0wU8FAmLif5oACgkQa+m8aLS0
8 wU8o2gv/VmbZp9uXEc4BQOIB4HPWSXb0Aa46ghD77v8YbYNOvmwPDMJ5yhF4YXz+
9 6waBqN/vrqqsQx/AuPT4jiT5+t3MpFI8O1I9XuzY3cTpTeBVnmobhKA98aDJvxZV
10 oT0/KoaxzsTDllOtkhl+a4Xts8YVlyy/4FWHBrQrmPV1OLemdpBuZmiYQQDS+jbW
11 2NjG5X20zqYgizNxxJvT5GyKPl8Osahq4joLvIl5HbPM+HUuQEUNkTZdJ1NBlzf3
12 5lRT/yiURyI+UlFM1MGtxjuJfPryk5PnjwbTTtIOEkMFZFgjcDfKA5NkCAfRVO56
13 sn85xD8rvXxsbiecuGahfyQ3Gij3kJmz7cO5kvcu/ntAjTk1hYCo8vG/p4ULDNd
14 hq+hugAzX7M+wbAvTiHHaAVUCZHyNcjIfozSFqxu/zaURWDseVrvcS8mDtyDNUMR
15 m0H0IjdZmY7HpnqNmOI94Cvt2bDRGwn8qYcNnGos3NxNltZQ8nMfpIyx+BHhavM6
16 JSHQ0mdC
17 =5lon
18 -----END PGP SIGNATURE-----
```

Firma digitale di Armando Diaz

Verifica della firma

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

I resti di quello che fu uno dei più potenti eserciti del mondo risalgono
in disordine e senza speranza le valli che avevano disceso con orgogliosa
sicurezza.
-----BEGIN PGP SIGNATURE-----

iQGzBAEBCgAdFiEEZuwm4z70r1kVVFkea+m8aLS0wU8FAmLif5oACgkQa+m8aLS0
wU8o2gv/VmbZp9uXEc4BQOIB4HPWSXb0Aa46ghD77v8YbYNOvmwPDMJ5yhF4YXz+
6waBqN/vrqqsQx/AuPT4jiT5+t3MpFI8O1I9XuzY3cTpTeBVnmobhKA98aDJvxZV
oT0/KoaxzsTDllOtkhl+a4Xts8YVlyy/4FWHBrQrmPV1OLemdpBuZmiYQQDS+jbW
2NjG5X20zqYgizNxxJvT5GyKPl8Osahq4joLvIl5HbPM+HUuQEUNkTZdJ1NBlzf3
5lRT/yiURyI+UlFM1MGtxjuJfPryk5PnjwbTTtIOEkMFZFgjcDfKA5NkCAfRVO56
sn85xD8rvXxsbiecuGahfyQ3Gij3kJmz7cO5kvcu/ntAjTk1hYCo8vG/p4UALDNd
hq+hugAzX7M+wbAvTiHHaAVUCZHyNcjIfozSFqxu/zaURWDseVrvcS8mDtyDNUMR
m0H0IjdZmY7HpnqNmOI94Cvt2bDRGwn8qYcNnGos3NxNltZQ8nMfpIyx+BHhavM6
JSHQ0mdC
=5lon
-----END PGP SIGNATURE-----
```

Firma digitale di Armando Diaz

```
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQGNBGLieu0BDADNDVqAEDCXzncL9QyurEzhlyTDdOIZt9dk46CKdT4B+xAPETiE
S+tSNBqhPCjmy5eikFa6nZv+ik2aNOVfPiZPLLS5DCQJnrtKT/6lpB9zVFRu+Ume
Mg2GauXhEUeqox2pS6VTTF1B05+wjU+AldSu/Im+35SERZrjmSOoHIPBSrJWibxS
EppyG8XA0t08+S5Ul4MDEZQr8ENqIsvgZjujyGEHhd16rpkAh8Go4Oof9wv6LfbK
7OqFpQsM66Rv/wRDzjBvFph1+tiZbOcJUaowkfXXNU0rbCcT25KwBCLD60/plzI2
olLc8uNXwfVIkvq3dFcmT49CMczIHT/RFR5qCvifdcF6Id//ukrAu6EHxJlsijbg
7u8AE8TXVQq2Jkp20/dUboEBvk6NIZ/TiQM8GfaR+yXQk7nIPk5DC2Q3u8GCosit
DeNw6oCBy5cR1B7DKC2Spl+KViRA4ui8fB6hAnUa7UXT6JewqppwzlNImcomrKkT
X0Ys7AsUlIENPY8AEQEAAbQfQXJtYW5kbyBEaWF6IDxhcm1hbmRvQGRpYXouY29t
PokB1AQTAQoAPhYhBGbsJuM+9K9ZFVRZHmvpvGi0tMFPBQJi4nrtAhsDBQkDwmcA
BQsJCAcCBhUKCQgLAgQWAgMBAh4BAheAAAoJEGvpvGi0tMFPS28L/0wxo8LzAI/s
bDCllbJzytqlaarvTc1eTGHwmq7AdgCfIgld5NnMAiPVuAtuSXhn4+Zw0nP4iDUG
I1EFy6NIXinBvQLgaidNfTg7u+sZSa9eFWfNI84cDrYhP8wPVQXMDNucG3PaPKsP
6Jpk+eKYmzPH0ONeowW2+YgFy+UUqp1rySwZNoVknRzXblWiAvlsrTqWqnmF5LVt
/Tm60lESR0seuS+w+Z/cHpIAzvJv9fDjI+BceYXZte5r8LGg5pZ/vSpwdzmqziuW
VWZ+5UbI02gEg03YNVAkGa8dV5VVyDN+qbtkxr4VgL6+k08vE/itDqVbmvjEpD9l
82eaq4SkVUBPIQKmp4yLMTQCC6Xjuznj3NfvPaVa8N02VBz4H9sfL8+L651I1TMo
fzf8g/zJM/QNiSxMHtL89N9XxmJ1PFCSN1RcolndVA7ibfgd2pEhFdeGGR2oKHTt
HVHnHWeRb7CbzxchcOGklhTuRXtko5o/2oAyVVPntSL2BIzUS06qM7kBjQRi4nrt
AQwAv6RF0r25eBNEVlIx4qnG5Yn49Izz/vQkQAUeUC+v/oAGWzMdtIbiQtZdx531
gp+WSsfrJ72Pcq9QdpRpBSMW25yCbcbWs+oSpbxhrpEVBFhUEm6qzSQRCBee9Aq/
mYMG7BwGKjYceCrPEnKFWT3pjHkwIcESmC40ak1WmVya5M18vWkFrfPepjj0wGtu
DXld9Q4GCO+zfQzdwarIhPyH24wDM85SB8jQDxdelLpPc7z+BAMZKNWlo2N62TzU
1RxIC3WCcbvWtoKDJ3XoHpWNFcolDZ5HiSxc4qQS8OiG3JBvBkMMyuCy8/jetY94
7jYho9asMZIAyIGR+ngELQSJNwzxBYYOEUO9745iqhqhurXdDVUwrf82q5fVVwBg
uc86gp3b/DVpvGmZfV0y/gFFliVw4lqWGZVbVorhNjxPyI4KFUQ0MFPH1825r4QB
UFJ6MFKdnS+54dk1FwxEdPvz2ZW1mt1dKHFGyrgllCE9D86XIcbvEtSOzYJaeBiU
7G4JABEBAAGJAbwEGAEKACYWIQRm7CbjPvSvWRVUWR5r6bxotLTBTwUCYuJ67QIb
DAUJA8JnAAAKCRBr6bxotLTBT/SoC/9BPyeY0cdq8mJtW34GVl7YOt47XfoBB218
WNM/D+Pl19B274+A/k3Wvhl0/Ge/zaoZeCFdnB7p6rjX+898jXFrYEMoHrlkbtMo
MrldJFHAYi7KfyDsHvyhRNCJ6j7Eg1eQtVlBzJXfa4PqYbKQY042cmagJVcMJW71
7krNPBlYPPKwWm7p5kTHJUChxtjmA/+SJvMwWIBUyHzzvlw2/vduLtO0IGsiJI+q
DsSsZCShR/Eev0x8btyDlQ1ctksBt8fh2cenr07f61RfGohftHdZ/yD9aiTX/xJQ
rYnBSD4j5w8bVROGCGboBS7NybXsfHaY3tZzJcuxWxbUCkVQy26yrhP2ApQcQOQM
5txSCl22fNr/9JFsP+t1Mo/T1me6odwfz6cF3vCG[illegible]0turrj2ciAd39njEwXGft
g4VjpDQwkBX+1CY+LKa2gcmPh7xzf5nZAJikaoI7E[illegible]M93HHIlNugGDyOOjd5U
SNgoQUC2bFlr+7HsL+D7tCejYvrT/C0=
=zKxt
-----END PGP PUBLIC KEY BLOCK-----
```

Chiave Pubblica di Armando Diaz

```
gpg --verify bollettino_vittoria.asc
gpg: Signature made gio 28 lug 2022, 14:22:50 CEST
gpg:                using RSA key 66EC26E33EF4AF591554591E6BE9E
gpg: Good signature from "Armando Diaz <armando@diaz.com>" [ult
```

Firma valida, controllabile da chiunque

Concetto semplice, ma declinato in Italia in maniera poco strutturata nei servizi:

- PEC
- Firma Digitale
- CIE
- SPID

Un piccolo sommario.
3 tipi di Identità Digitale:

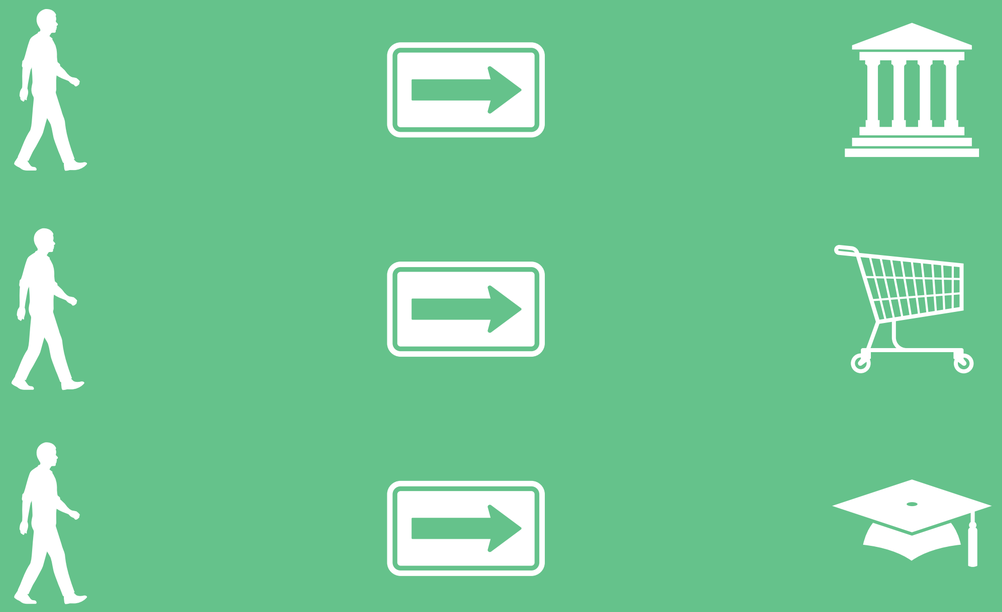
- **Modello Centralizzato**
- **Identità Federata**
- **Identità Decentralizzata**

Credito a Marco Marinelli:
https://mirror.xyz/0x859481eE6854f4078dd19D50Dcf10919DFaE6786/nsRw3sb029D1jjBWc9I010bpqlXXYs-VOEBa2xRwfo0

Modello Centralizzato

Username + Password

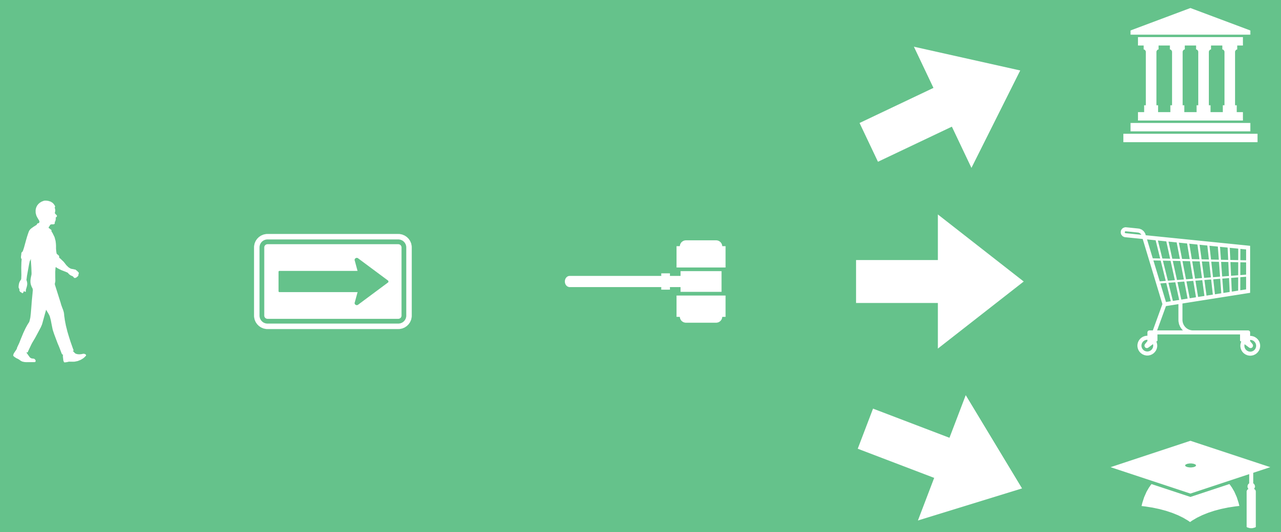
- Credenziali diverse per ogni servizio
- Informazioni salvate dal gestore del servizio

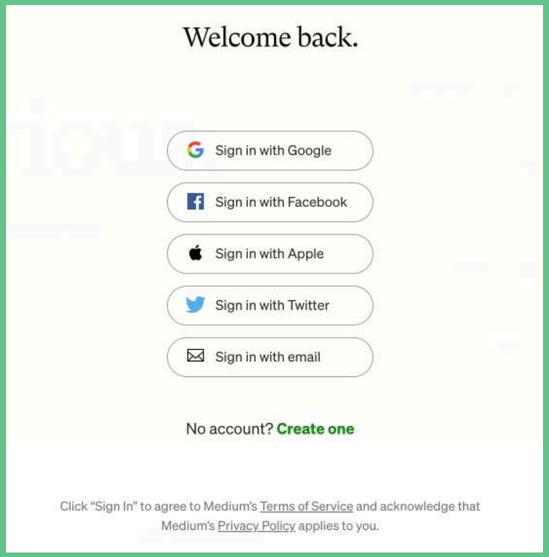


Identità Federata

Identità fornita da un Identity Provider (IdP)

- Stessa identità può essere usata per servizi diversi (Single sign-on)
    - Esempio: SPID, Login con Facebook, Google etc...
- Informazioni salvate dall'IdP





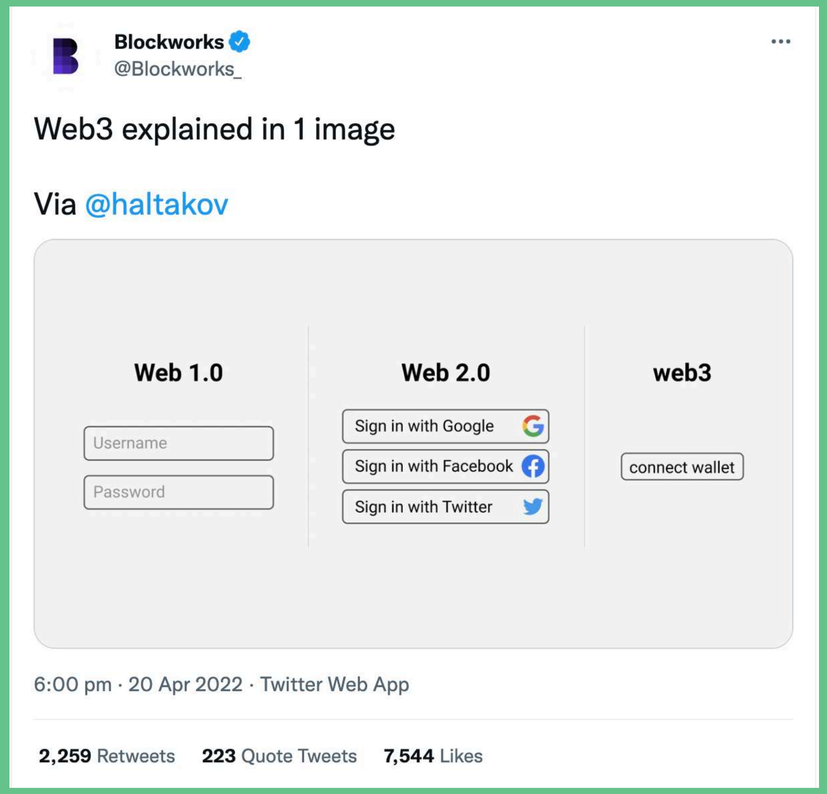
Esempio: login a Medium

Identità Decentralizzata

Identità in pieno controllo dell'utente

- L'utente ha un wallet (portafoglio digitale) che contiene "Verifiable Credentials" emesse da enti certificati (e.g., Governo, Università)
- Scambio di informazioni direttamente tra utente e richiedente
    - Solo informazioni necessarie (e.g., prova di essere maggiorenne)
    - Non ci sono intermediari

Prossimo decennio



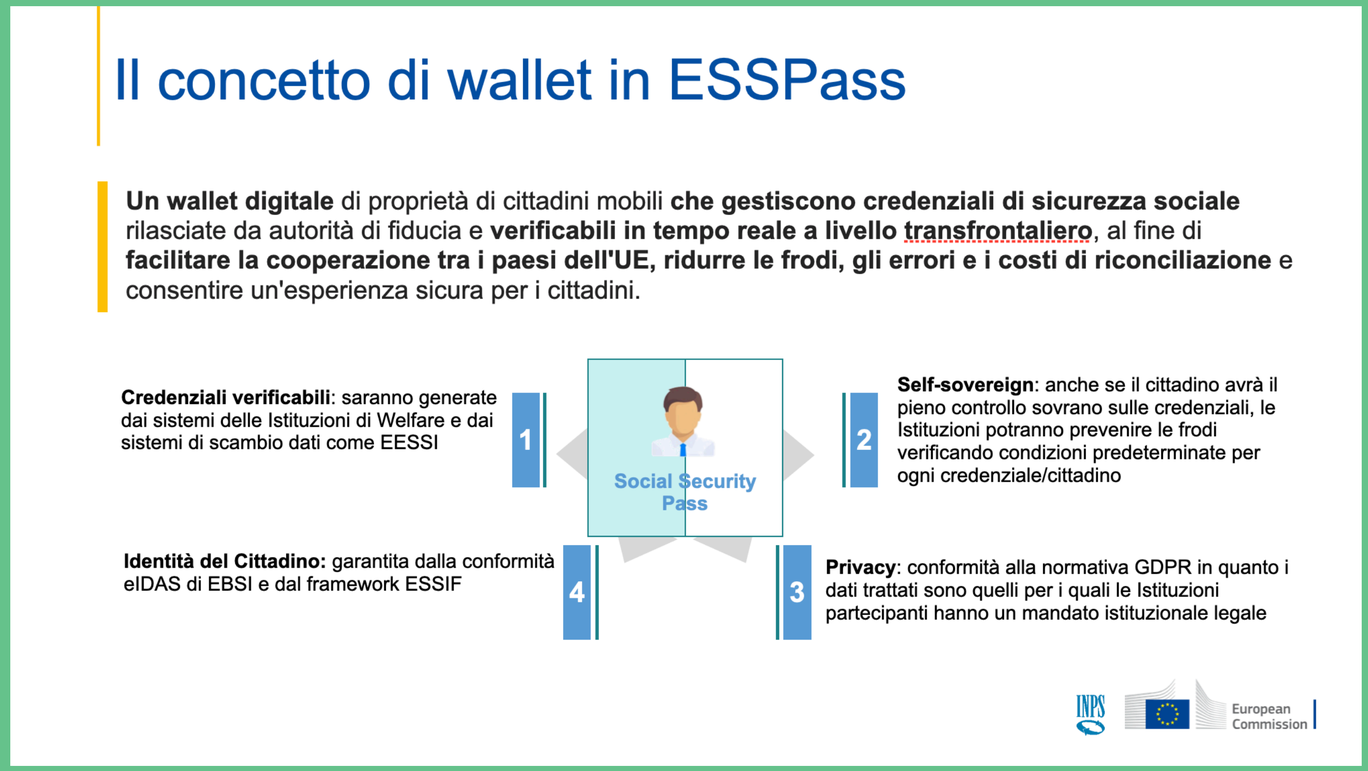
Credito a Vladimir Haltakov e Blockworks: https://twitter.com/blockworks_/status/1516808921276723208

European Self-Sovereign Identity Framework (ESSIF)

Identità decentralizzata basata su tecnologie Blockchain

- Lavori portati avanti da EBSI (European Blockchain Services Infrastructure) e in Italia da IBSI (Italian Blockchain Services Infrastructure)
- Progetti pilota: Diplomas e ESSPass (European Social Security Pass)
- INPS capofila degli enti promotori di questa evoluzione

INPS in primissima linea per il futuro dell'Identità Digitale e i suoi usi



Credito a Stefano Cascone e squadra di lavoro INPS

Q&A

vincenzo@inps.it

@vincenzo

@vincenzo