
Protezione e privacy dell'identità SPID
Problematiche e soluzioni per i cittadini
e gli operatori sanitari.
bit4id

Protezione e privacy dell'identità SPID

Problematiche e soluzioni per i cittadini e gli operatori sanitari

AGENDA

- Introduzione
- Contesto
- Opportunità e problematiche
- Soluzioni e suggerimenti
- Casi d'uso

Luca Scotto
lsc@bit4id.com
lucascotto@gmail.com

Introduzione

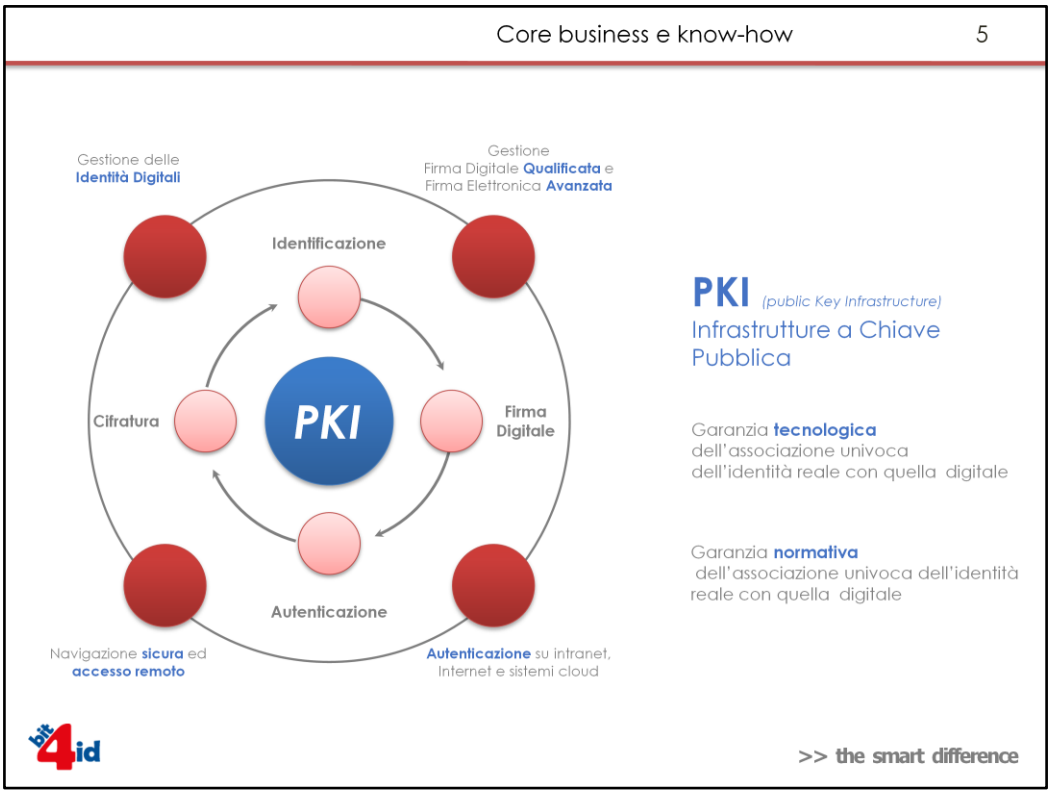
Luca Scotto
Product manager
Corporate security

- **Fondata** nel 2004, capitale privato
- **Missione**: prodotti e sistemi di sicurezza "real plug&play"
- **Fattori critici di successo**: Innovazione, Esecuzione, Eccellenza
- **Tecnologie**: PKI (Public Key Infrastracture), smartcard
- **Principali Mercati**: Italia, Spagna, Portogallo, Grecia, Regno Unito, Turchia, Ungheria, Polonia, Bulgaria, Romania, Macao, Perù, Equador, Guatemala, Columbia

bit4id >> the smart difference

Riferimenti progettuali SAML/SPID:

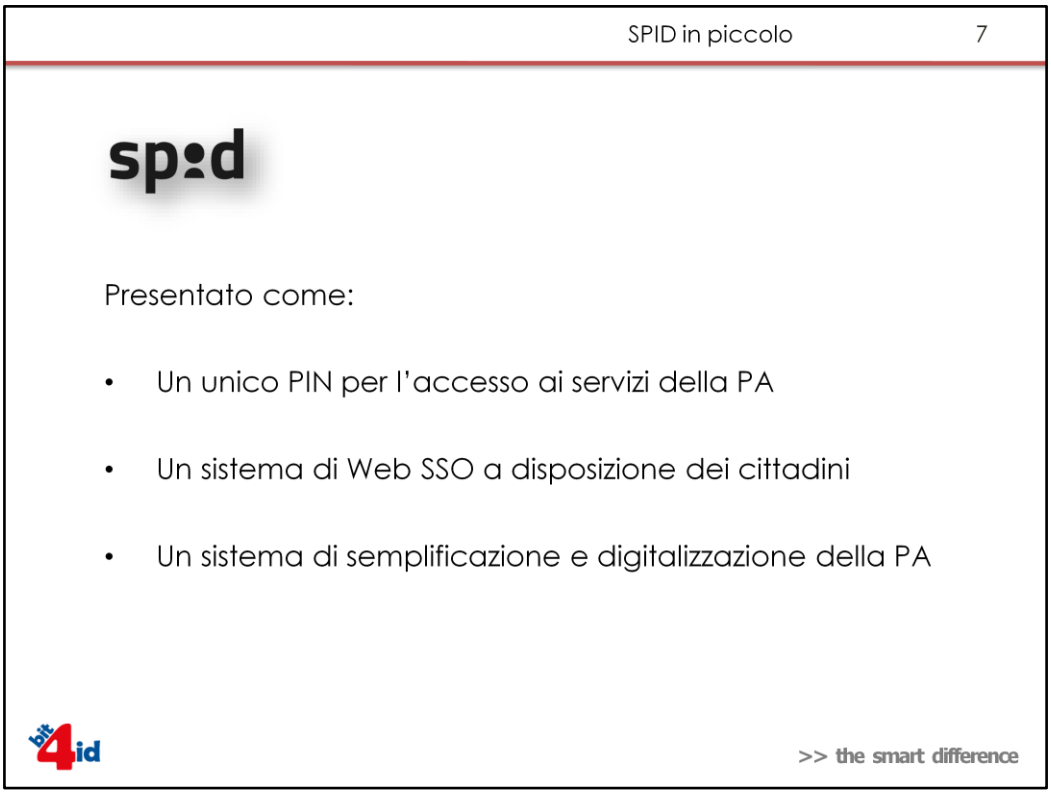
- Identità federata SAML(shibbolet/cas): CUP Regione Campania
- Identità operatori sanitari : Progetto FDCOS
- Identità federata applicativa SAML (SAML 2.0): Progetto Security Framework - Regione Veneto



Tematica PKI per identificazione, firma digitale e cifratura:

- **Unicità** dell'identità digitale
- Gestione tramite **certificati digitali** e C.A.
- **Indipendenza** dal formato tecnologico
- **Tracciabilità**
- **Attendibilità** ed **Integrità** delle informazioni
- **Sicurezza** e **Privacy** garantita
- Tecnologia **stabile,** interoperabile, basata su **standard** internazionali
- Rispetto delle **normative** e validità in un contesto **giuridico**

Contesto



Le chiavi in cui SPID viene presentato

Il quadro d'insieme

Anagrafe Unica Digitale : Anagrafe centralizzato in sostituzione di 8.000 anagrafi territoriali in modo da rendere semplici e centralizzate richieste di cambio residenza e certificati anagrafici

Pagamenti Elettronici (pagoPA) : Il sistema dei pagamenti elettronici pagoPA permette a cittadini ed imprese di effettuare pagamenti in modalità elettronica verso pubbliche amministrazioni e gestori di servizi di pubblica utilità.

Open Data : Gli Open Data sono dati pubblici che devono essere pubblicati in maniera che sia facile il riutilizzo. Facilitazione dell'adozione di standard ed accessibilità ai dati.

Linee Guida siti web PA : Le linee guida dei siti web della PA sono un sistema condiviso di riferimenti visivi relativi al design dei siti.
Hanno lo scopo di migliorare e rendere coerente la navigazione e l'esperienza del cittadino online.

Competenze digitali : La Coalizione per le Competenze digitali è lo strumento principale della Strategia per la crescita digitale per il sostegno alle iniziative di alfabetizzazione digitale del paese.

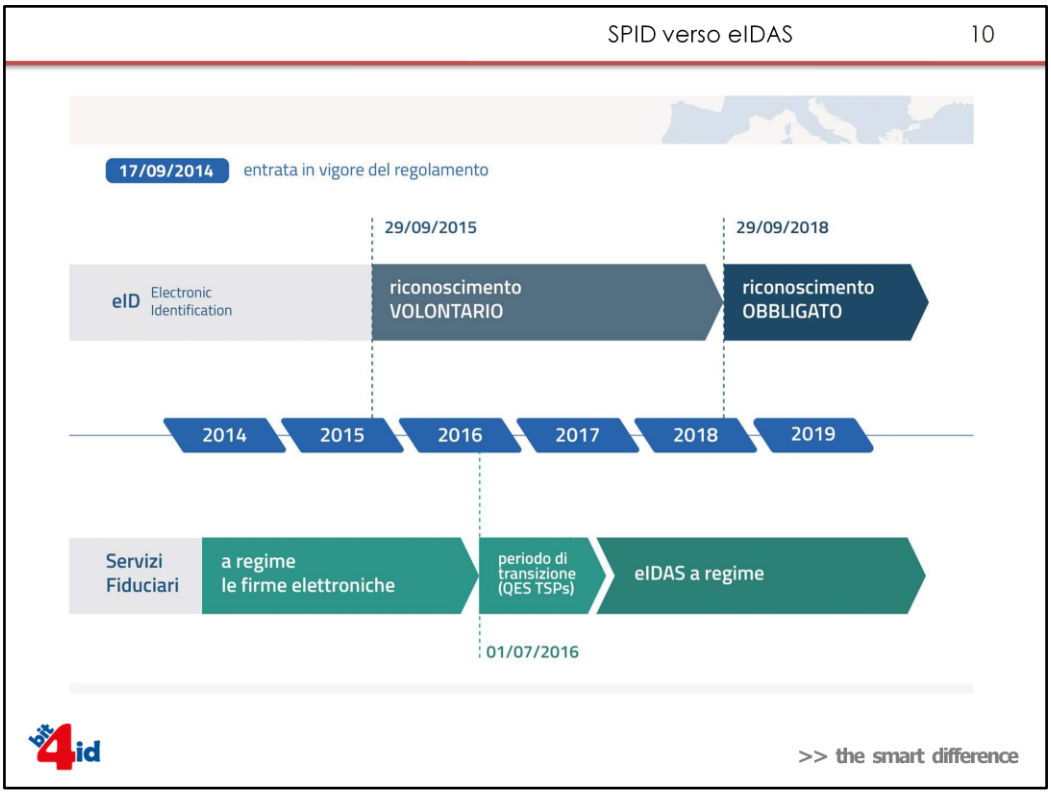
SPID verso eIDAS

"SPID è stato disegnato in conformità al Regolamento eIDAS, e rappresenta una delle iniziative trasversali della **Strategia per la Crescita Digitale 2014-2020**."

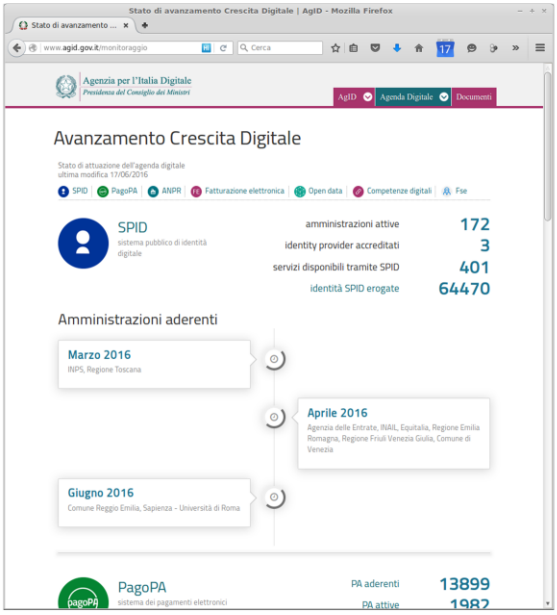
bit4id >> the smart difference

SPID vs CNS

Le tecniche e protocolli su cui si basa SPID sono già stati sperimentati a livello europeo e adottate dai progetti sperimentali Stork e Stork II (Secure idenTity acrOss boRders linKed).



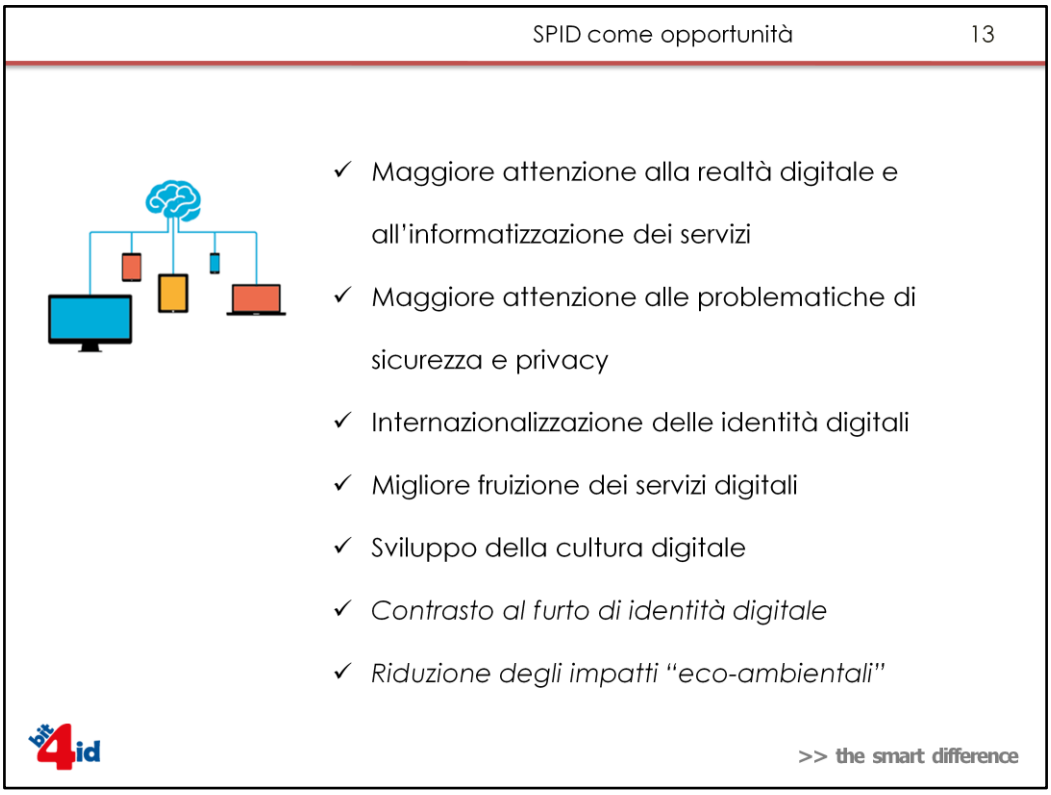
SPID e eIDAS hanno un percorso organizzato e condiviso che impatta l'intero sistema PA non solo del paese Italia, ma l'intera Europa.
Il percorso è quindi diverso dall'impostazione che a suo tempo fu della CIE o CNS.



bit4id

>> the smart difference

Opportunità



Riferimento e riflessione sugli articoli "ufficiali" pubblicati.
Al di là dei proclami, l'impatto di SPID si misura sull'attenzione alla sicurezza e problematiche associate anche da chi prima ignorava tali contesti.
Maggiore interessamento e talvolta conoscenza del problema della gestione delle identità arriva anche ai "piani alti".
Non è un caso che la stessa PA, traino anche del settore privato, sia andata in questa direzione.
L'introduzione della figura del Data Protection Officer (DPO) non è casuale ma ben in linea ai modelli internazionali.

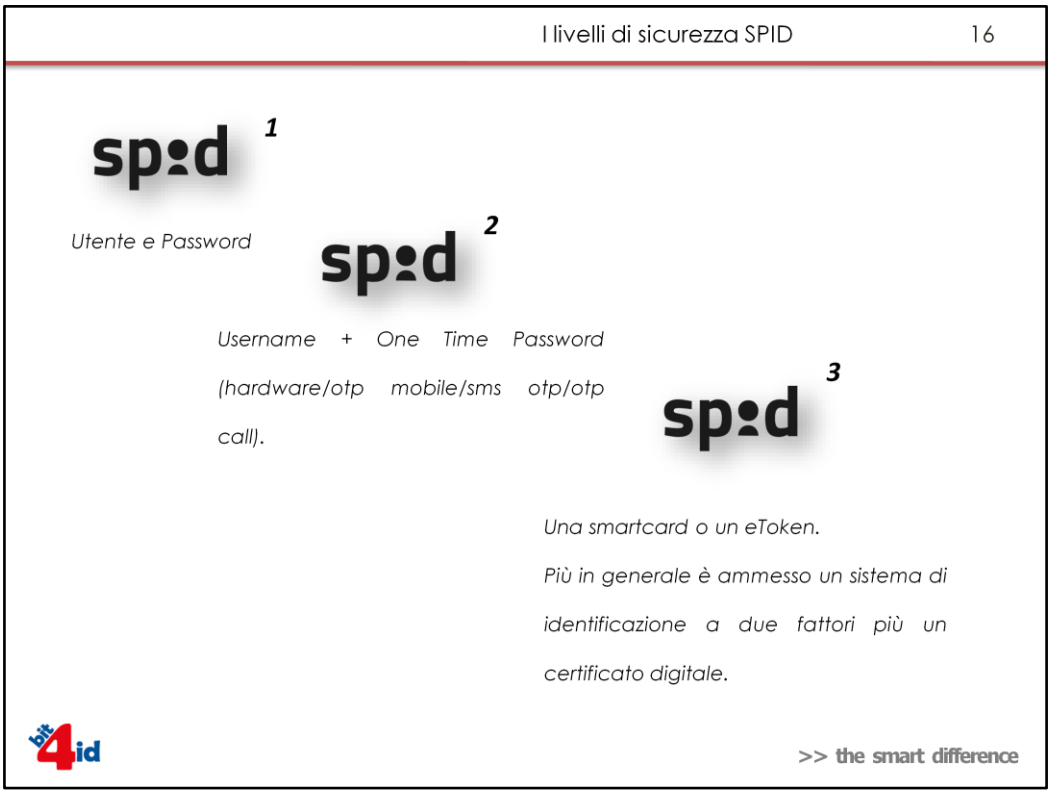
Il direttore AgID Antonio Samaritani, individua SPID come strumento sicuro riassumendo tre punti importanti:

- *C'è un processo di identificazione fisica dell'utente certo.*
- *Il processo è definito e concordato col garante della privacy a tutela dei dati personali.*
- *Si utilizzano protocolli e logiche di sicurezza affinché l'identità non venga rubata e falsificata.*

bit4id >> the smart difference

Riferimento agli articoli ufficiali su internet.

Problematiche



I livelli di sicurezza utilizzabili

Non tutti i livelli sono equivalenti.

SPID è realmente inattaccabile se utilizzo una smartcard.

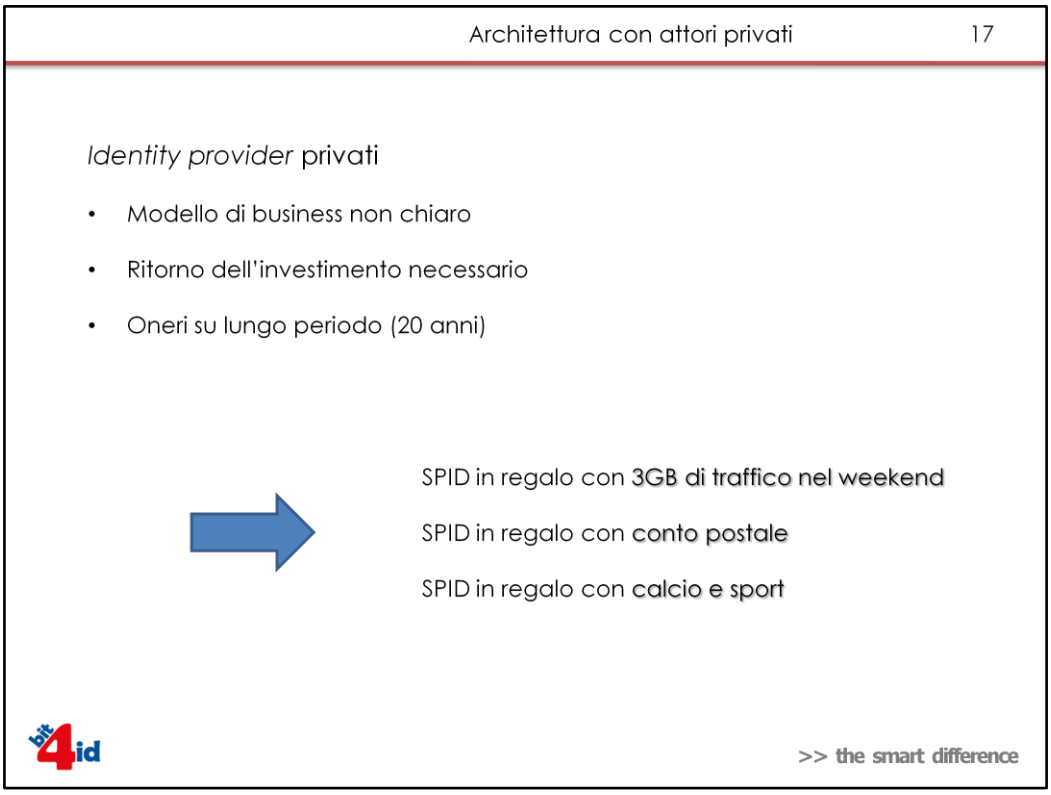
Se uso un “level 3” che utilizza chiavi in un HSM a cui accedo con un OTP uso nei fatti un level 2.

In un sistema di accesso il livello di sicurezza è dato dal fattore più debole, non quello più alto.

Se in un PC o in uno smartphone si accede con il fingerprint ma ho, in emergenza, la possibilità di accedere anche con un PIN di 5 caratteri, il livello di sicurezza sarà dato dal PIN e non dal fingerprint.

Un attaccante batte sempre sull’anello più debole.

Bisogna fare attenzione a delegare al sistema SPID tutti i problemi di sicurezza e privacy.



Mercificazione
Il ritorno dell'investimento è uno dei fattori più critici se nel processo entrano aziende private.
Tanti dubbi e poche risposte anche dagli addetti ai lavori.
Gli attori sono TIM / INFOCERT / POSTE ITALIANE

Soluzioni

Cosa gli esperti e gli addetti ai lavori dovrebbero suggerire.

Utilizzo consapevole di SPID per gli operatori sanitari:

- Utilizzo di identità di **terzo livello**
- Utilizzo degli **attributi** di ruolo
- **Uniformità** delle applicazioni e servizi aziendali
- **SSO** con identità SPID
- **Formazione**

bit4id >> the smart difference

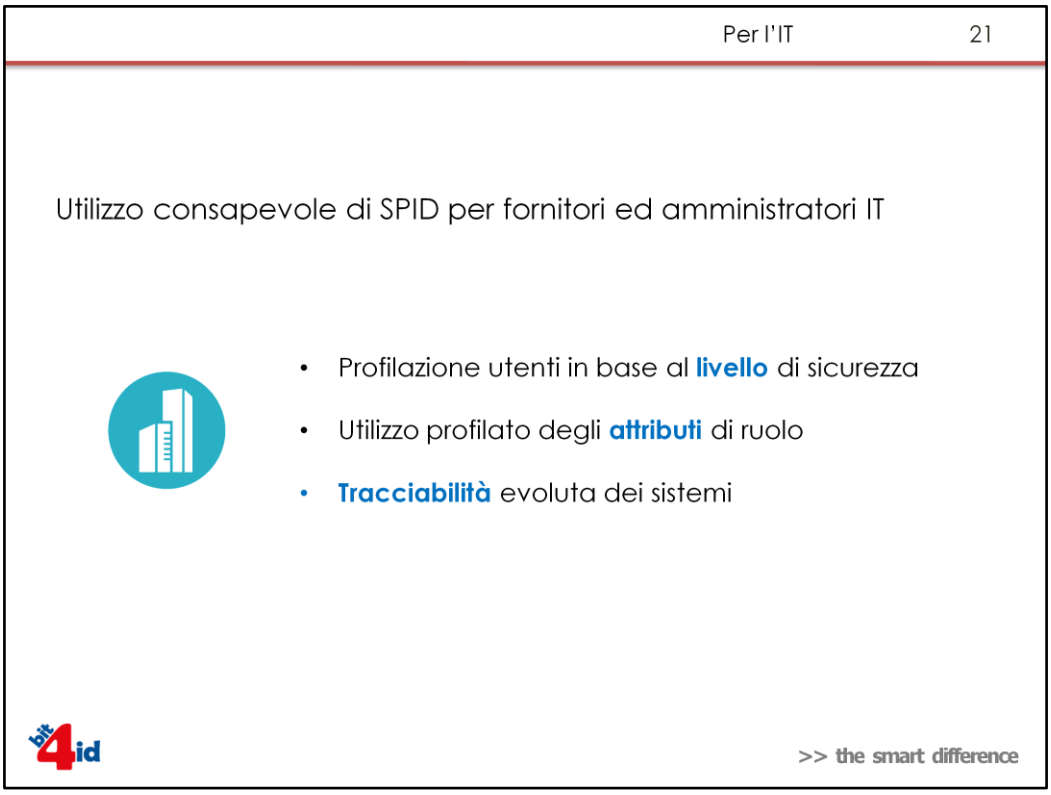
Gli operatori sanitari sono utenti “anomali”.
Per esigenze lavorative devono infatti accedere e gestire dati sensibili. Col tempo potrebbero avere identità SPID da utilizzare nel loro lavoro quotidiano.
In un modello d’uso corretto, un operatore dovrebbe avere un’identità SPID dissociata da quella di privato cittadino.

Utilizzo consapevole di SPID per e con gli utenti:

- Educazione alla sicurezza
- **Consapevolezza** nell'uso dei livelli disponibili
- Non mercificazioni delle identità
- **Uniformità** delle applicazioni e servizi offerti
- Utilizzo di app dedicate o browser hardenizzati
- smartToken per il digital divide

bit4id >> the smart difference

I cittadini sono liberi di utilizzare o meno l'identità SPID.
Chi offre servizi deve prevedere che l'accesso possa essere fatto da persone non necessariamente informatizzate, eventualmente avverse all'uso spinto della tecnologia e alla diffidenza in un sistema di identità che gli viene offerto da un privato.
La mercificazione è un arma a doppio taglio con cui è difficile fare previsioni.



Sposando un modello di autenticazione federato aumenta la necessità di gestire al meglio i servizi offerti utilizzando adeguatamente i livelli di sicurezza e gli attributi. Ha inoltre sempre maggiore rilievo l'uso di strumenti di tracciabilità.

Casi d'uso

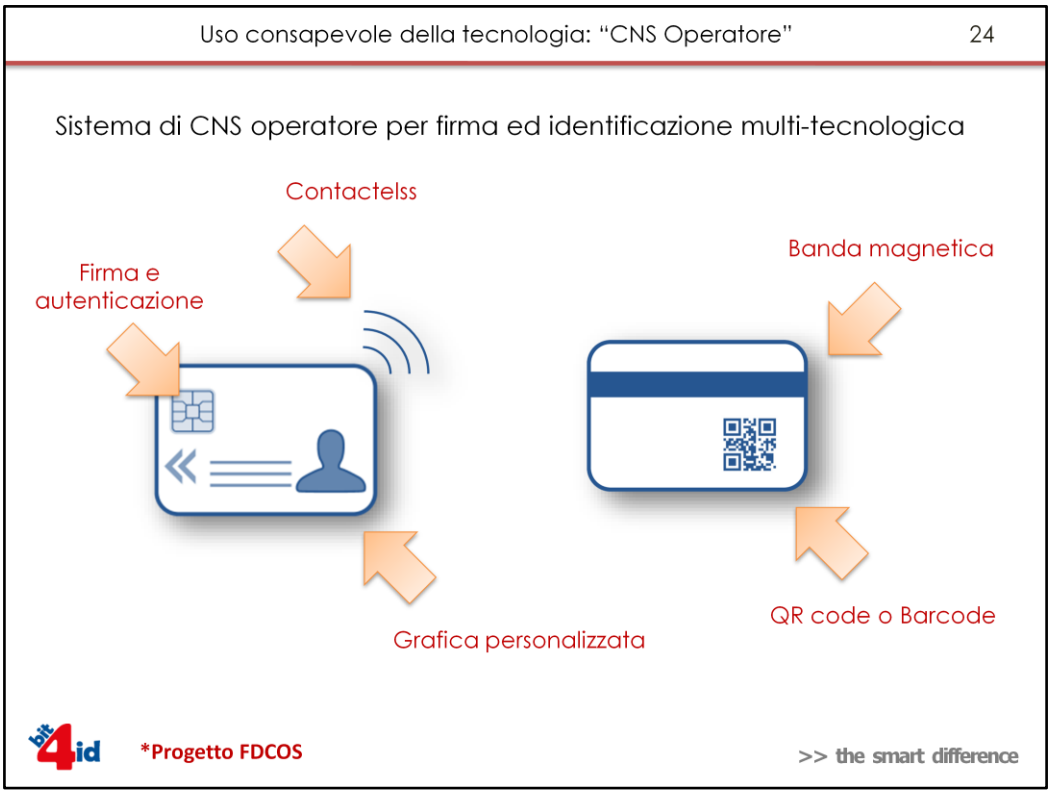
Ovvero impariamo da sperimentazioni e progetti su tecnologie affini.

Sistema di CNS operatore per firma ed identificazione.

Alcune considerazioni sugli operatori sanitari:

- Non sempre hanno uno smartphone aziendale
- Non necessariamente devono utilizzare uno smartphone privato
- Non dovrebbero utilizzare la propria identità di cittadini per fini lavorativi
- Hanno il diritto di essere salvaguardati in termini di responsabilità sui sistemi che utilizzano

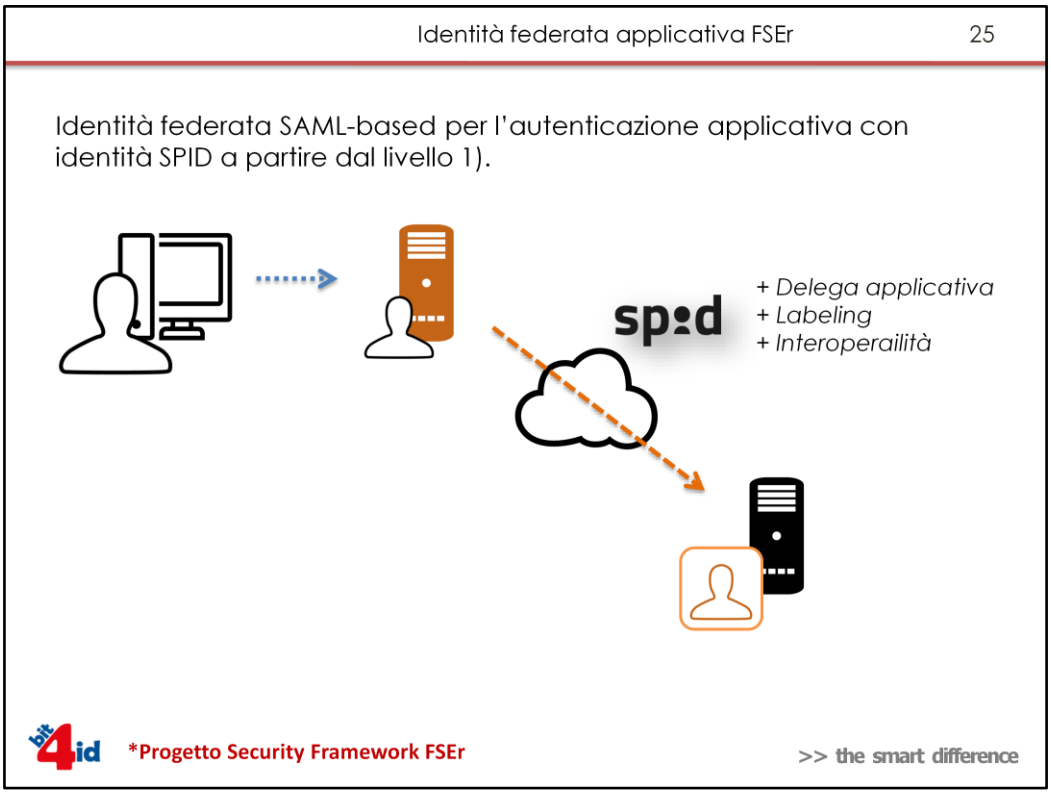
*Progetto FDCOS



L'utilizzo di un unico badge, ossia una smartcard, può essere una soluzione agevole per avere SPID ad uso lavorativo ma anche come unico strumento per:

- Timbrare
- Pagare la mensa
- Accedere al parcheggio
- Accedere al PC
- Utilizzare l'identità SPID di livello 3

Così come per la CNS, anche per SPID, serve motivare l'utente finale che ha un unico strumento per tutto.



Un modello evoluto di autenticazione applicativa federata.
Non sempre è applicabile un livello di sicurezza elevato. E' però possibile combinare sistemi di sicurezza in modo da promuovere il livello di sicurezza globale.
I meccanismi di "delega applicativa", labeling e certificati digitali applicativi possono agire anche su sistemi dove si utilizza la più semplice username/password.
E' inoltre possibile mantenere l'interoperabilità tra sistema spid e sistemi di identità federata locale/regionale rendendo trasparente architetture di questo tipo.

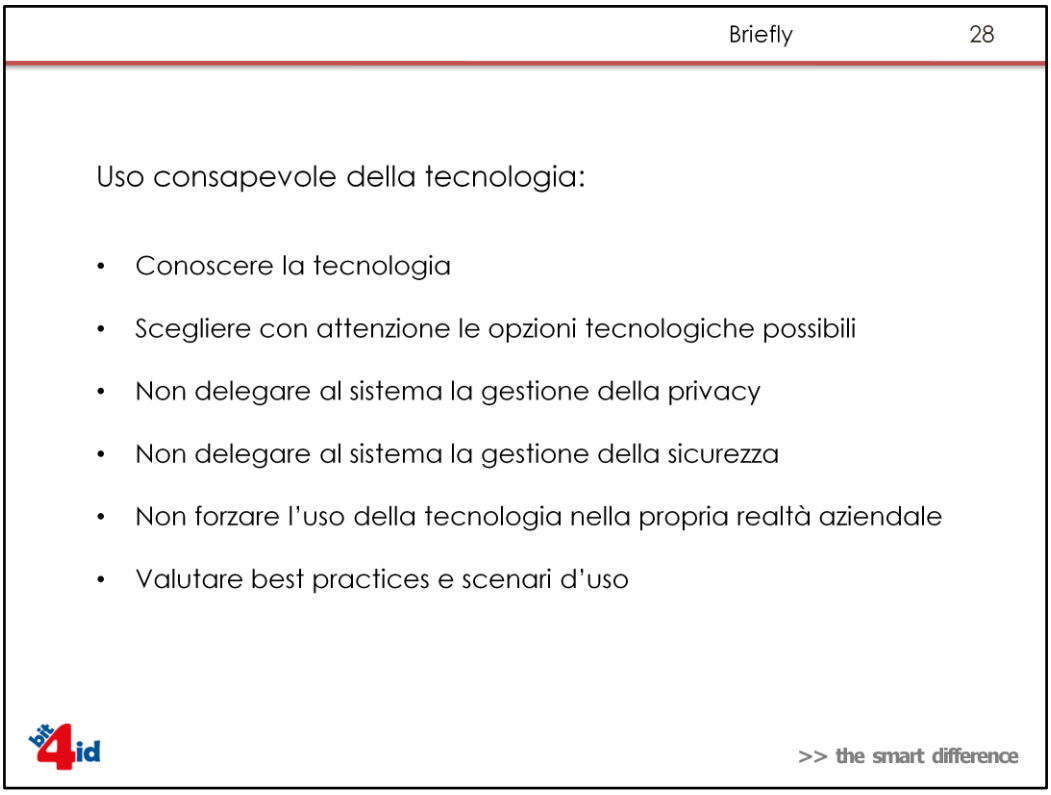
Identità federata SAML-based per l'autenticazione applicativa con identità SPID a partire dal livello 1).

*Progetto Security Framework FSEr

>> the smart difference

In figura i componenti messi in campo per la gestione di un sistmaa di identità federata.

In conclusione



In conclusione

Lo Spid, come ogni processo informatico, richiede l'organizzazione e la pianificazione di misure e metodologie di sicurezza atte a garantire la protezione e la privacy dei cittadini e degli operatori, che per esigenze lavorative, dovranno adottarlo.

I primi sono soggetti non necessariamente informatizzati, i secondi gestiscono ed operano informazioni sensibili.

In uno scenario di cybercrime, che non conosce frontiere territoriale, l'applicazione di un sistema di identità digitale pubblico deve necessariamente confrontarsi con le realtà tecnologiche più avanzate, standard internazionali e best practices.

Strumenti e soluzioni valide esistono, e sono già applicate in ambito sanitario e bancario con successo con tecnologie affini.

L'uso consapevole della giusta tecnologia rappresenta l'unico approccio possibile in uno scenario di identità digitale pubblico su larga scala.

Riferimenti

Luca Scotto
Product manager
Mobile: +39 328 722 42 14
E-mail : lsc@bit4id.com
E-mail : lucascotto@gmail.com
50C1 3842 12AD 908B 8772 D65D C17B 17B5 B550 E564

www.bit4id.com

Bit4id nel modo

ITALY
Naples:
Via Diocleziano, 107
80125 Naples – Italy
info.it@bit4id.com
Tel. +39 081 7625600
Fax. +39 081 19731930

Rome:
Via Tirone, 11
00146 Rome
Tel. +39 06 32803708
Fax. +39 06 99335481

Milan:
Tel. +39 02 430019163
Fax. +39 02 45500675

SPAIN
Barcelona:
Barcelona Advanced Industry Park
C/ Marie Curie, 8-14
08042 Barcelona - Spain
Tel: +34 902 60 20 30

UNITED KINGDOM
2 London Wall Buildings
London Wall,
London EC2M 5UU - UK
Tel. +44 1422 570673
Fax. +44 20 78553780

PERU
Mártir Olaya, n° 169
Oficina 406 (Miraflores) - Lima
(Perú)
Tel: +(51) 1 242 9994
info.pe@bit4id.com

>> the smart difference