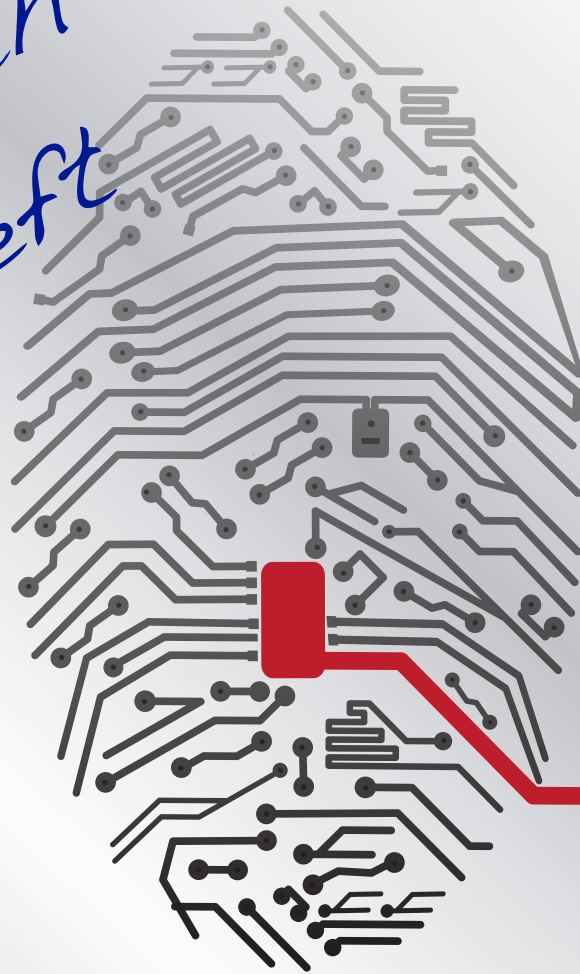


*the effective approach
against identity theft*

Sandro Fontana
CISSP, CISA, CISM, L.A. 27001, C|CISO

sandro.fontana@gt50.org

Q-ID



PROTECTING YOUR PRIVACY

prefazione

Ci sono due tipi di crittografia in questo mondo:

- 1 la crittografia che fermerà la vostra sorellina dal leggere i vostri file,
e crittografia che fermerà i più potenti governi dal leggere gli stessi file.*

- 2 Se prendo una lettera, la chiudo in una cassaforte, nascondo la
cassaforte da qualche parte a New York, quindi ti chiedo di leggere la
lettera, questa non è sicurezza*

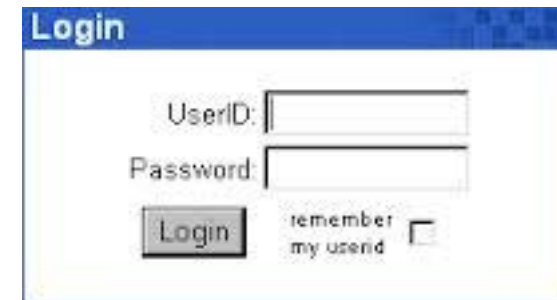
questa è oscurità

D'altra parte

*se prendo una lettera e la chiudo in una cassaforte, quindi ti consegno la
stessa cassaforte con le sue specifiche di progetto, insieme ad un centinaio
di casseforti identiche con le loro combinazioni, in modo che tu ed i
migliori scassinatori del mondo possiate studiare il meccanismo di
chiusura, e dopo tutto questo, non riuscite ancora ad aprire la prima
cassaforte e leggere la lettera,*

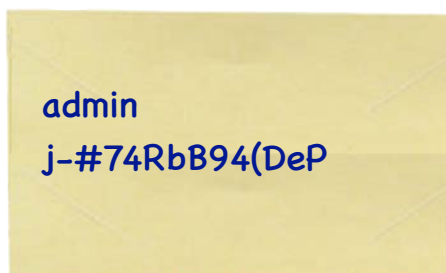
questa è sicurezza

L'accesso ai sistemi online è tipicamente regolato da credenziali di accesso costituito da coppie userid e password.



La crescita di questi servizi online mette gli utenti in una situazione critica, senza nemmeno renderli consapevoli di questo: la password è diventata l'identità elettronica di un individuo e deve essere attentamente protetta.

Una password lunga e complessa è una password forte, ma ...
le password complesse e complesse sono molto difficili da ricordare.



admin
j-#74RbB94(DeP

Gli utenti in genere utilizzano le password in base a dati personali, che sono facili da ricordare, ma anche da indovinare.

Queste sono le 5 password più comuni scelte dagli utenti di tutto il mondo nel 2014(*)

- 1) 123456
- 2) password
- 3) 12345
- 4) 12345678
- 5) qwerty

(*) <http://splashdata.com/press/worst-passwords-of-2014.htm>

Quello che è ancora più pericoloso, è il fatto che molte persone usano la stessa password sia per i loro account personali e di lavoro.

Tutto questo porta al furto di identità elettronica



Le vittime scoprono troppo tardi che sono stati derubati della loro identità, cominciano a ricevere richieste di pagamento per iscrizioni non rimborsabili o addebiti per beni che non hanno acquistato.

In alcuni casi, inoltre, si può rischiare di perdere la reputazione di buon pagatore e avere difficoltà a raggiungere nuovi prestiti o mutui.

Il furto di identità elettronica è un problema molto serio.

Colpisce tutta la comunità: ciò significa danni diretti o indiretti per i cittadini, le imprese e le istituzioni, sbarrando il passo alla fiducia sull'utilizzo dei servizi on-line, il che significa meno eGovernment, meno efficiente meno progresso,.

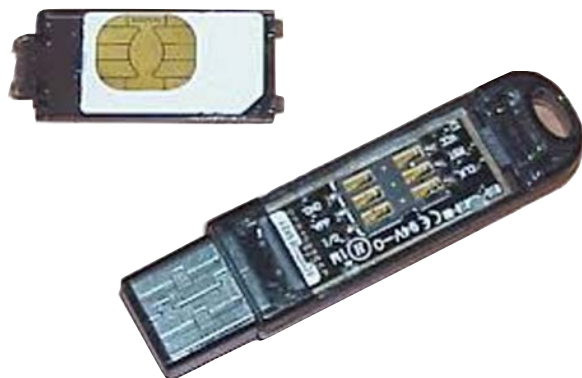


L'unica possibilità che rimane, è quella di utilizzare meccanismi di accesso che consentono all'utente di gestire in modo semplice e sicuro la propria identità elettronica.

Il fatto che il sistema debba essere facile da usare è molto importante: utilizzando una soluzione complessa da capire, è facile commettere errori.

Smart Card

hanno bisogno di un lettore fisico e un driver software locale; inoltre richiedono la distribuzione e la gestione dei certificati



USB stick

richiedono un driver software locale; inoltre richiedono la distribuzione e la gestione dei certificati

La One-Time-Password (OTP) è un meccanismo di sicurezza, in genere incarnato in un piccolo apparato [token], che permette di accedere a una rete oppure ad un servizio, fornendo all'utente una password che può essere utilizzata una sola volta.



La One-Time Password è una forma di autenticazione forte, basata su algoritmi proprietari (RSA, Vasco, Gemalto) o Open Standard (OATH)



È un dispositivo sicuro, semplice da utilizzare, semplice da implementare dalle aziende, ed è infatti sempre più utilizzato e consigliato.



Per queste ragioni, le prime istituzioni che hanno cominciato ad attuare questo meccanismo di sicurezza, sono state le banche.



La tecnologia si è diffondendo ad altre aree; il sistema è considerato così sicuro, che oggi viene utilizzato per attivare la generazione di una firma digitale da remoto.



Naturalmente, più entità utilizzano questo meccanismo, più token OTP gli utenti dovrebbero portare con sé.

Ovviamente, non è così.

Nel migliore dei casi, i token vengono conservati in luoghi "sicuri", con il risultato che, quando gli utenti hanno la necessità di utilizzarli, i token non sono disponibili.

Inoltre dover gestire due o più token diversi, può portare a errori e confusione.



Paradossalmente, le stesse caratteristiche che hanno fatto il successo di questi sistemi One-Time-Password, stanno creando un problema: sempre più spesso gli utenti si trovano con diversi token hardware a disposizione e questo fatto provoca spesso confusione sul loro uso.

i costi di gestione della distribuzione,
della sostituzione, per il furto, i
malfunzionamenti, la perdita ...



Su numeri di utenti significativi,
anche il solo impegno economico per
l'acquisto dei token hardware,
può diventare
un vincolo non facilmente superabile.

visionary
innovation



una singola App per smartphone,
universale, interoperabile, sicura,
basata su standard pubblici

ed in grado di gestire un elevato numero di token OTP virtuali

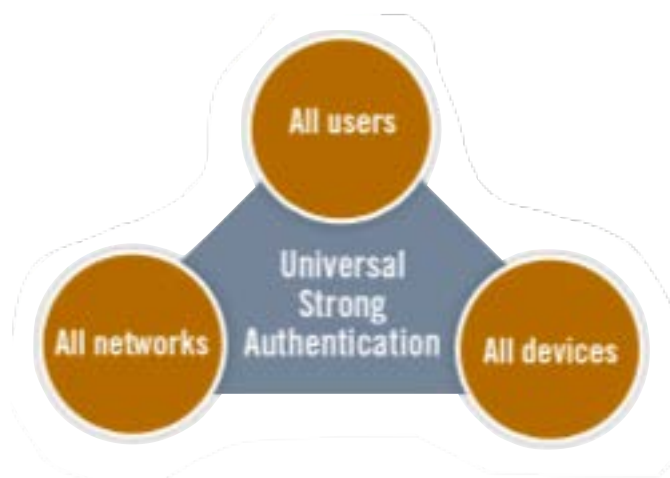
universale: qualunque tipo di smartphone

interoperabile: qualunque tipo di servizio

sicura: basata sui più robusti algoritmi di crittografia standard



... ed è gratuita



Allo scopo di mantenere lo stesso livello di sicurezza della tecnologia OTP hardware, per mantenere i costi al minimo e superare i problemi di gestione contemporanea di più token, la piattaforma Q-ID™ offre all'utente un App su smartphone, in grado di gestire una o più schede, ognuna contenente un token OTP virtuale (standard OATH)

Il vantaggio di utilizzare l'App Q-ID™, è quello di essere grado di gestire -con una singola applicazione- differenti token OTP, per accedere a diversi sistemi, reti o servizi.



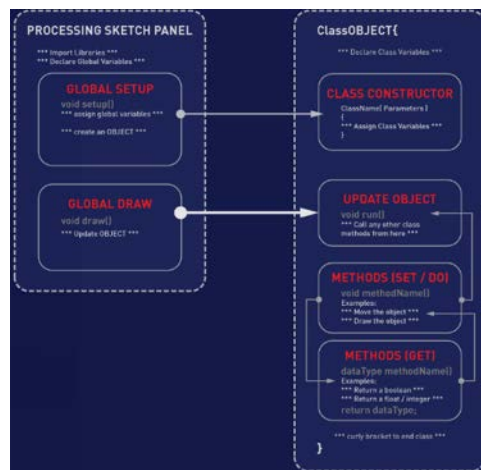
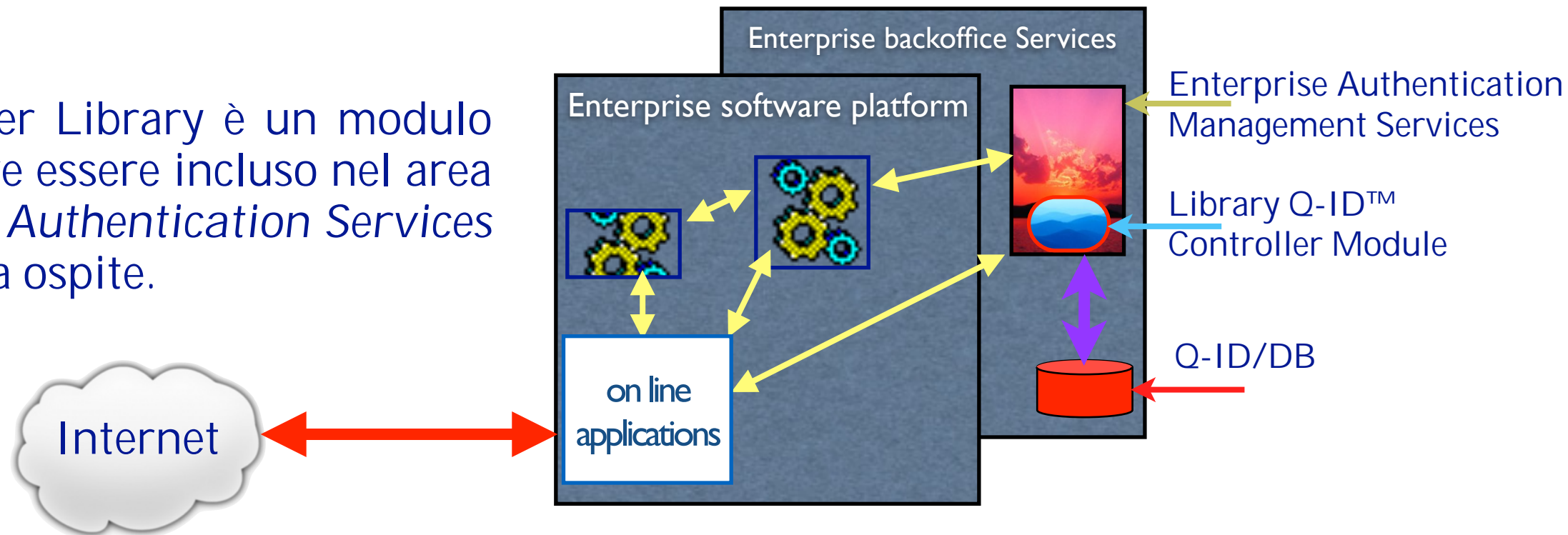
L'accesso alle funzioni della App, è subordinata all'inserimento di una unica MasterPassword di attivazione, al fine di garantire l'utente da uso fraudolento dell'App Q-ID, in caso lui/lei perda il suo smartphone.



L'App Q-ID, è anche in grado di gestire i segreti personali dell'utente
(di più su questo, nelle prossime slide)

Oltre l'App Q-ID™, la piattaforma è composta di un modulo software centrale:
Q-ID™ Controller Library

Q-ID™ Controller Library è un modulo software che deve essere incluso nel area degli *Enterprise Authentication Services* della Piattaforma ospite.



Questo modulo fornisce agli sviluppatori di software dell'Azienda, tutte le funzioni per gestire gli elementi di OTP, dalla fase di iscrizione (tramite *SQCode aidSystem*), alle verifiche delle OTP, agli eventi di sincronizzazione, alla gestione di licenze d'uso nel loro ciclo vitale.

... ed è gratuita

Il livello di sicurezza è il massimo garantito dall'applicazione di questi standard:

- OATH (Open Authentication); (*)
- AES256 (symmetric Encryption);
- RSA1024 (electronic signature);
- SHA256 / BCrypt (cryptographic digest);

Inoltre, la fase di generazione sicura dei seed OTP, inizia all'interno dei sistemi dell'azienda Q-ID, utilizzando dispositivi hardware certificati Common Criteria EAL+.

Quando questi seed vengono acquisiti da *Q-ID™ Controller Library*, vengono ulteriormente trasformati all'interno e sotto il controllo della Applicazione di Autenticazione dell'Azienda che sta utilizzando la Piattaforma Q-ID™.

In questo modo, nessuno all'esterno dell'Azienda -neppure noi che abbiamo generato i seed di base- può avere il controllo o informazioni sulle OTP(**).

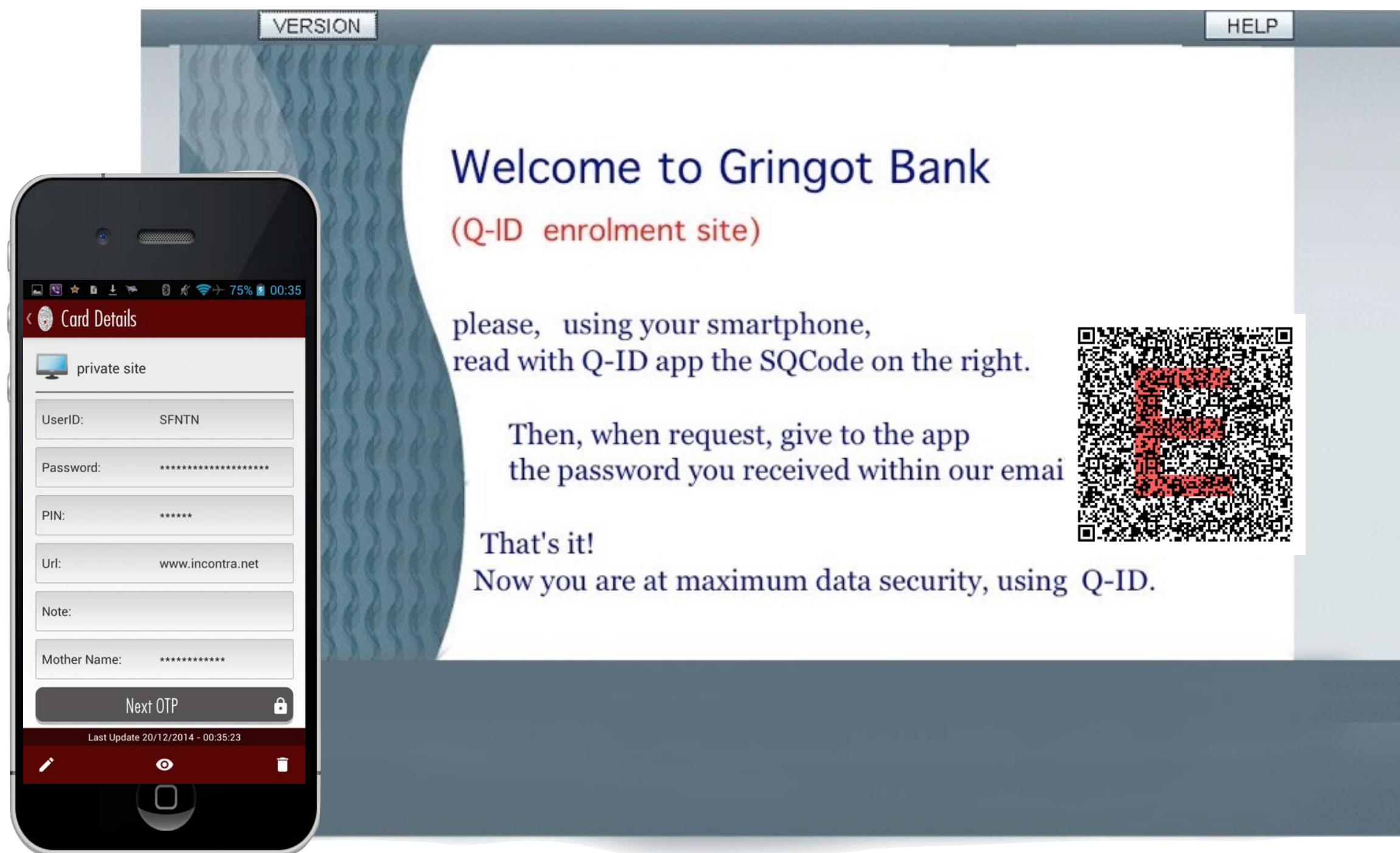
(*) https://www.schneier.com/blog/archives/2011/03/rsa_security_in.html

(**) <http://blogs.gartner.com/mark-diodati/2011/06/02/the-seed-and-the-damage-done-rsa-securid/>

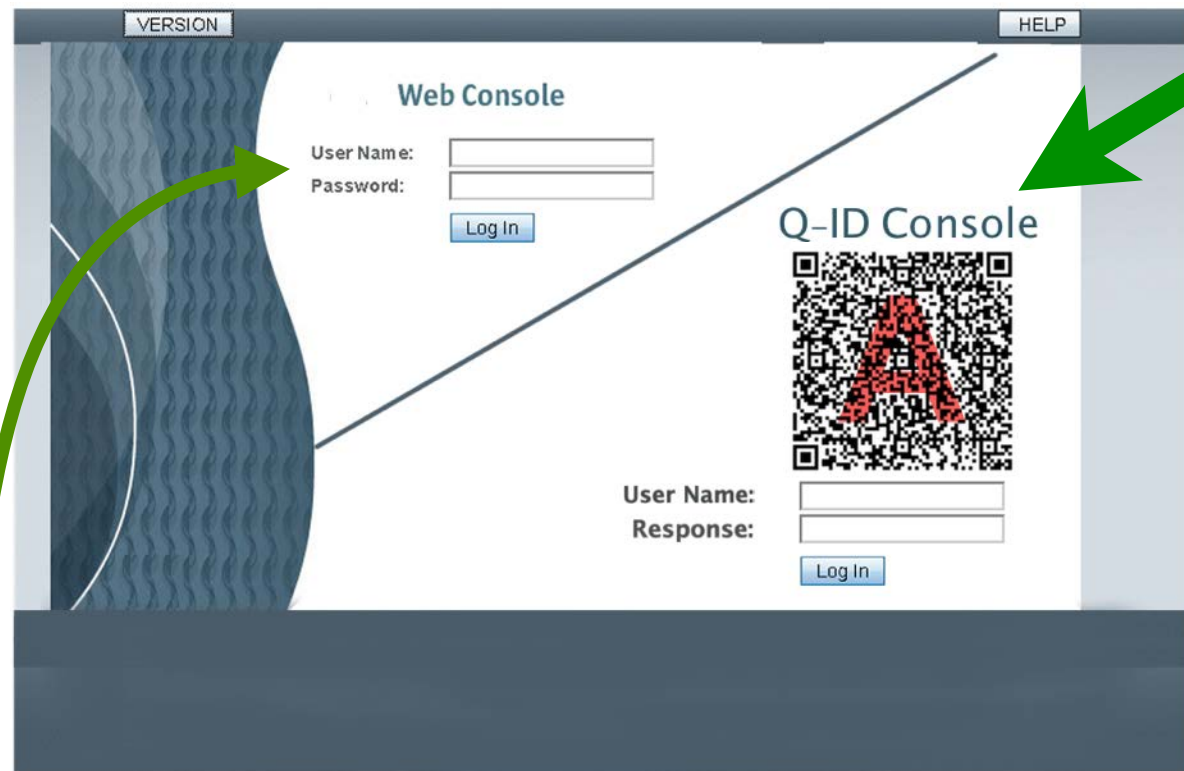
L'assenza di costi per l'App Q-ID™ e Q-ID™ Controller Library insieme al costo contenuto della licenza per numero utenti (lato server), consente di affrontare l'uso della OTP, anche in presenza di un gran numero di utilizzatori.

Software	q.ty	price
Library Q-ID™ Controller	1	free
Maintenance (year)	1	free
App Q-ID™	1	free
Maintenance (year)	1	free

Single User License Costs			
Total User	1st year	2nd year 10% off	3rd year 20% off
10	6,00 US\$	11,40 US\$	16,20 US\$
100	3,00 US\$	5,70 US\$	8,10 US\$
1.000	1,84 US\$	3,50 US\$	4,97 US\$
10.000	1,18 US\$	2,24 US\$	3,19 US\$
100k	0,75 US\$	1,43 US\$	2,03 US\$
1M	0,45 US\$	0,86 US\$	1,22 US\$
5M	0,30 US\$	0,57 US\$	0,81 US\$
10M	0,25 US\$	0,48 US\$	0,68 US\$



Usando l'App Q-ID™, l'utente legge il codice SQCode E_Type e l'App genera una nuova scheda contenente un Token Virtuale OTP

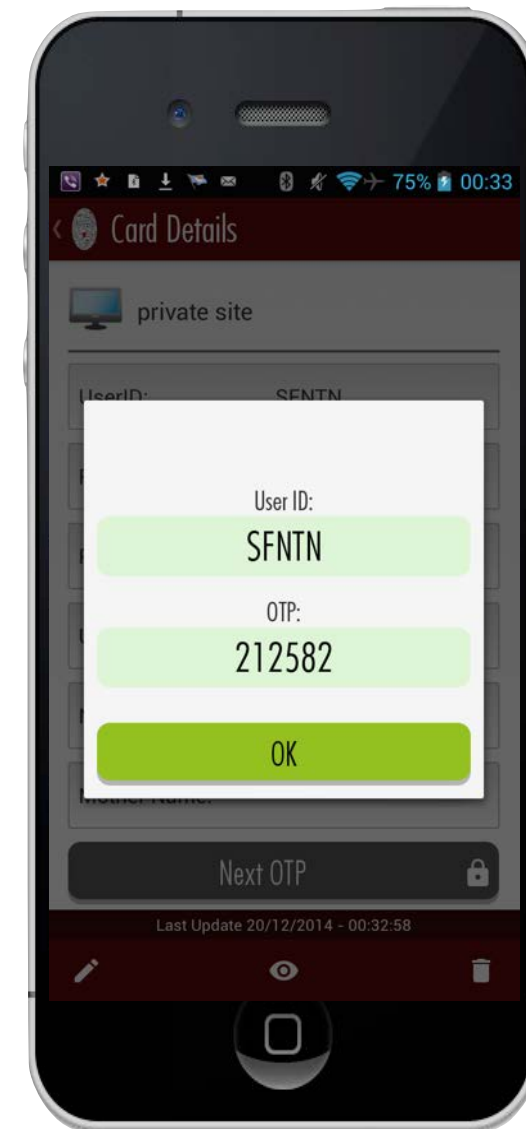


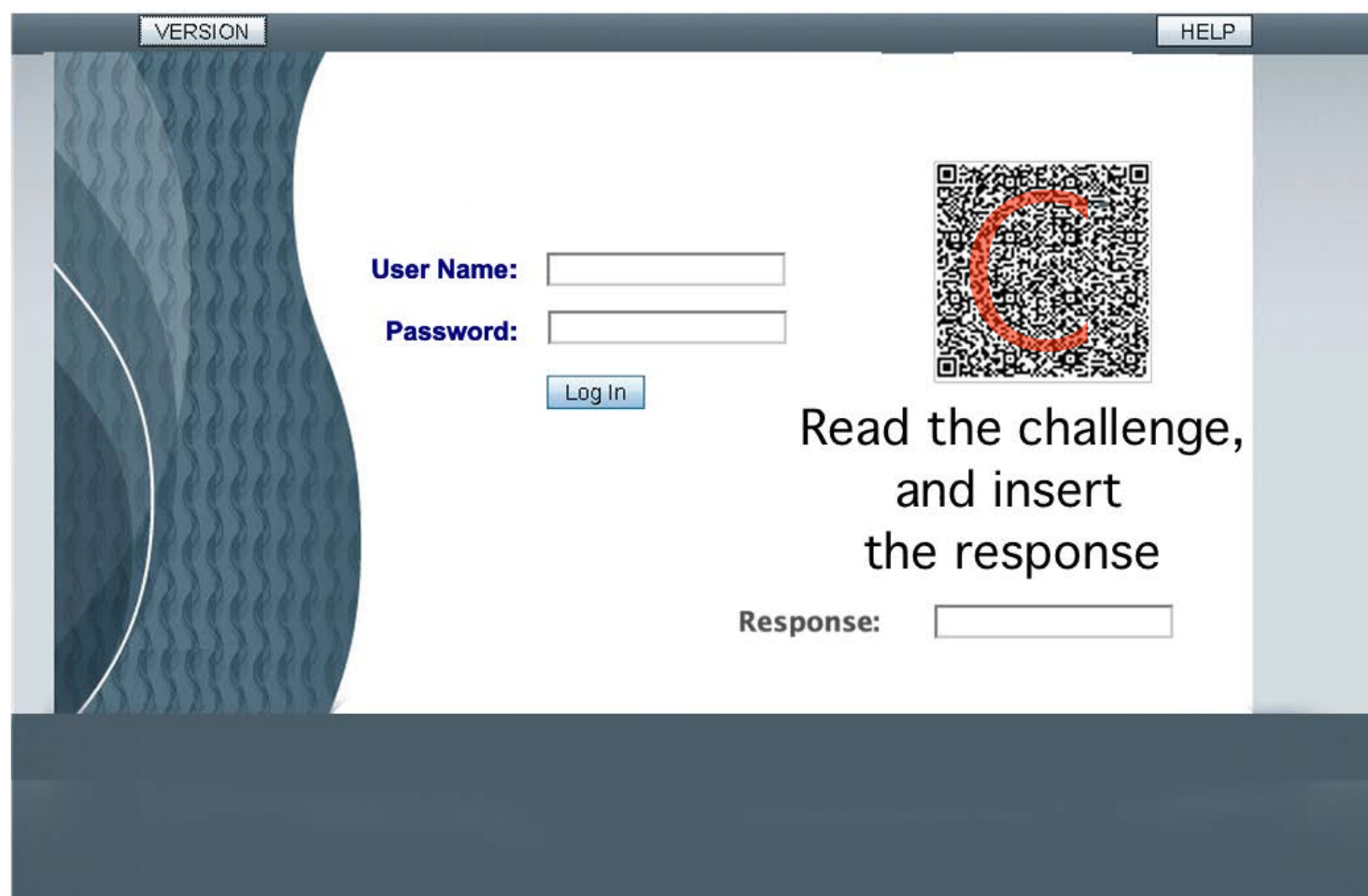
Nel caso di siti che sfruttano SQCode *aidSystem*, l'utente può leggere, per mezzo dell'App Q-ID™, l'SQCode A_TYPE .

Dopo aver decodificato l'SQCode A_Type, l'App mostrerà lo UserID associato a questo servizio insieme alla prossima OTP.

In questo modo si evitano errori aiutando l'utente nella ricerca della scheda corretta.

Nei siti che preferiscono non utilizzare SQCode *aidSystem*, sarà cura dell'utente selezionare la corretta scheda all'interno dell'App Q-ID™, quindi richiedere alla applicazione stessa la generazione di una nuova OTP.





The screenshot shows a web-based login interface for Q-ID. At the top, there are two buttons: 'VERSION' on the left and 'HELP' on the right. The main area contains a login form with the following elements:

- User Name:** A text input field.
- Password:** A text input field.
- Log In:** A blue button.
- Challenge:** A square QR code with a large red 'C' overlaid on it.
- Instructions:** The text 'Read the challenge, and insert the response' is displayed below the QR code.
- Response:** A text input field labeled 'Response:'.

Qualche volta è necessario scambiare i dati tramite un canale non sicuro, oppure c'è un alto rischio di fishing (man-in-the-middle)

In questi casi anche una OTP non dovrebbe essere trasferita in chiaro al server che eroga il servizio richiesto.

Il protocollo challenge/response, risolve questi problemi.

Dopo aver decodificato l'SQCode Type_C, l'App Q-ID™ mostra lo UserID, il tipo di richiesta, le informazioni associate a questo codice e la firma applicata come un numero da 8 digit.

Questa procedura, protegge l'Utente da truffe e dall'attacco detto "man-in-the-middle".

VERSION HELP

bank transfer

Insert Review Confirm

Checking Account: UK67H3981062723000000003231 Dennis Richie

Receiver: Brian Kernighan

IBAN: FR40K2301200023000213002132

Amount: 31.250,00 max 250.000,00€ al giorno

Date: 16/10/2014

Note: From Aho for co-authorship of the AWK programming language

Continue

INSERT YOUR SIGNATURE HERE

Bonifico Bancario (esempio)

Per confermare un bonifico,
la banca presenta all'utente
un SQCode Type_C
(SQCode aidSystem)

L'App Q-ID™ i dati da firmare [*Data To Be Signed* (DTBS)] leggendo l'SQCode Type_C, quindi mostra i dati all'utente, chiedendo la generazione di una OTP.

Tramite questa OTP e della rappresentazione del DTBS, crea una Firma Elettronica Avanzata (nella forma di una sequenza di caratteri)
(Questo metodo evita l'attacco *man-in-the-browser*)

L'utente inserisce questa firma all'interno di un campo previsto e completa la transazione; l'applicazione (in questo caso nella Banca), verificherà la firma per controllare l'integrità dei dati e l'autorizzazione dell'Utente.

Potrebbe presentarsi il caso di che un utente che, per una ragione o l'altra, non voglia utilizzare il proprio smartphone con l'applicazione Q-ID™



Uno dei vantaggi della Piattaforma Q-ID™, nell'utilizzo di uno standard come OATH, è quello di poter operare anche con Token OTP hardware in parallelo ai Token OTP virtuali.

Q-ID™ Controller Library, gestisce indifferentemente e contemporaneamente, i Token Virtuali gestiti dall'App Q-ID™ ovvero Token hardware, conformi allo standard OATH





L'App Q-ID™
è in grado di interfacciarsi
con altri ambiente sicuri
e
è anche in grado di gestire
i segreti personali degli utenti



Nella scelta di un software per la gestione di token OTP virtuale, dobbiamo ricordare che gli utenti continueranno ad avere altri sistemi su cui dovranno accedere.

Sistemi che continueranno ad avere una UserID ed una Password, come credenziali di accesso.



In questa situazione quello che è necessario è una soluzione che possa aiutarvi a generare password robuste e contemporaneamente possa memorizzarle per voi in modo sicuro:
una cassaforte virtuale per i vostri segreti

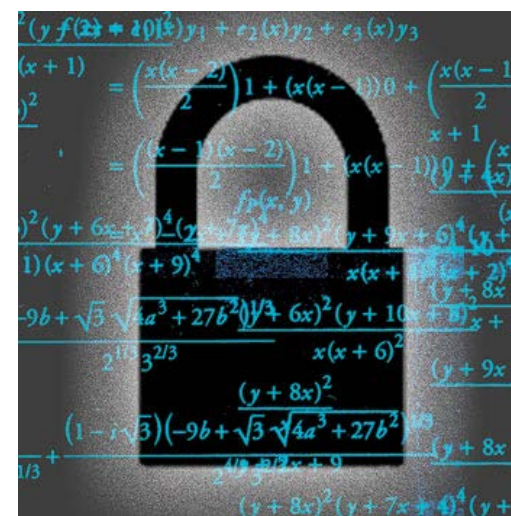


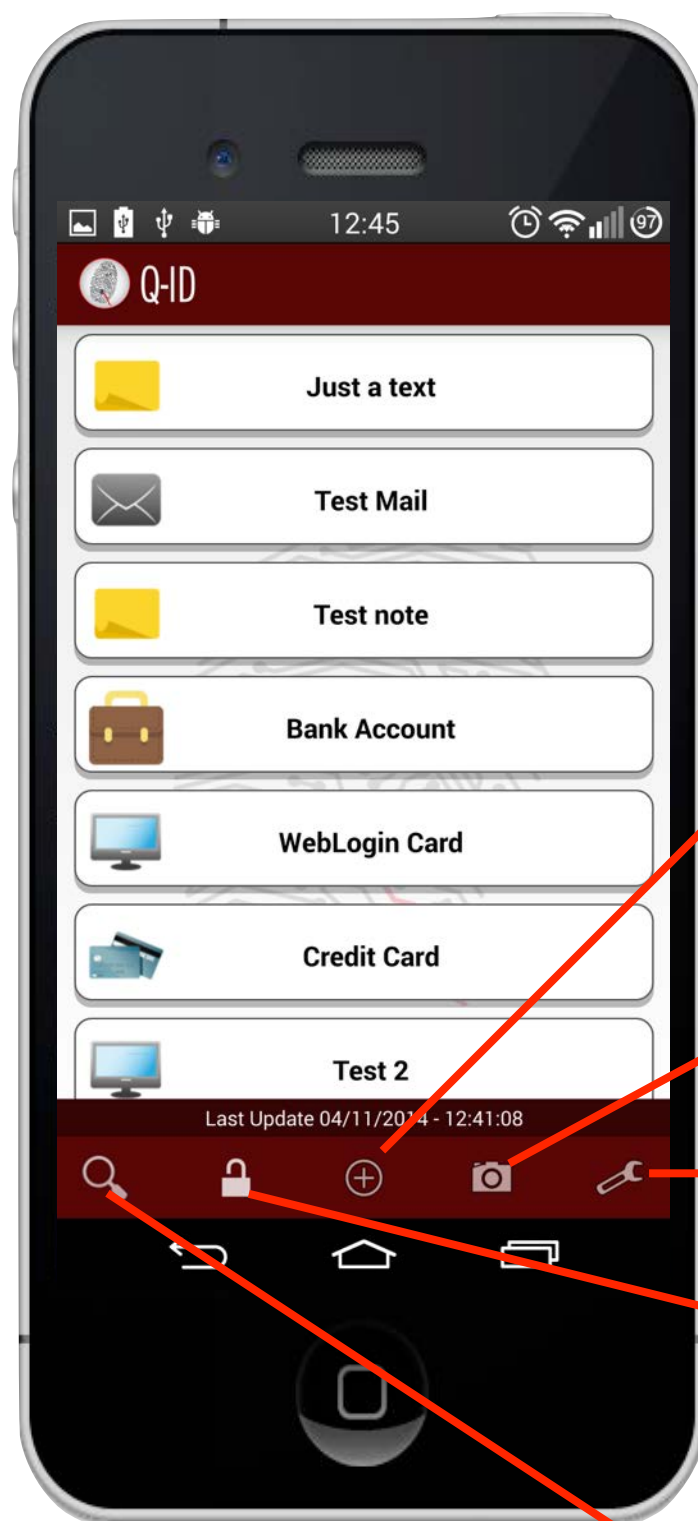
In questo contesto, l'App Q-ID fornisce un importante contributo alla sicurezza di identità elettronica di un utente, anche quando questo utilizza semplici sistemi userid/password.

Q-ID consente di semplificare l'intero processo di registrazione e di ricerca di password e dati, consentendo di recuperare facilmente le password necessarie per accedere ai siti Web e applicazioni.

L'App Q-ID ha la capacità di aiutare l'utente nella creazione di password robuste e consente di memorizzare altre informazioni riservate come i PIN delle carte di credito ed altro ancora.

Tutte le informazioni gestite dall'App Q-ID, sono codificate usando il più forte algoritmo di crittografia simmetrica attualmente disponibile come standard: AES 256





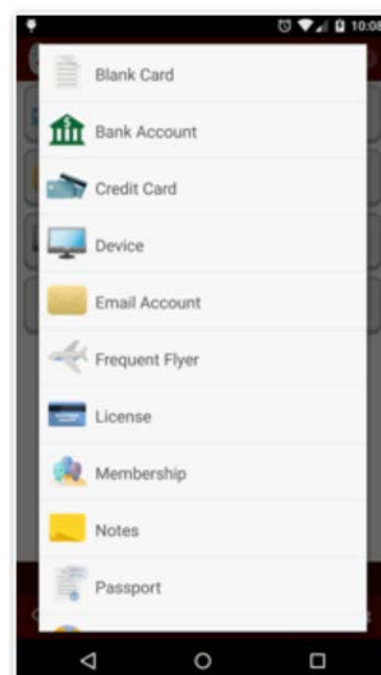
crea una nuova scheda
da vari template

attiva camera
per lettura SQCode

settings

codifica/decodifica testo
in clipboard

ricerca full text



aggiungi un campo
alla Card

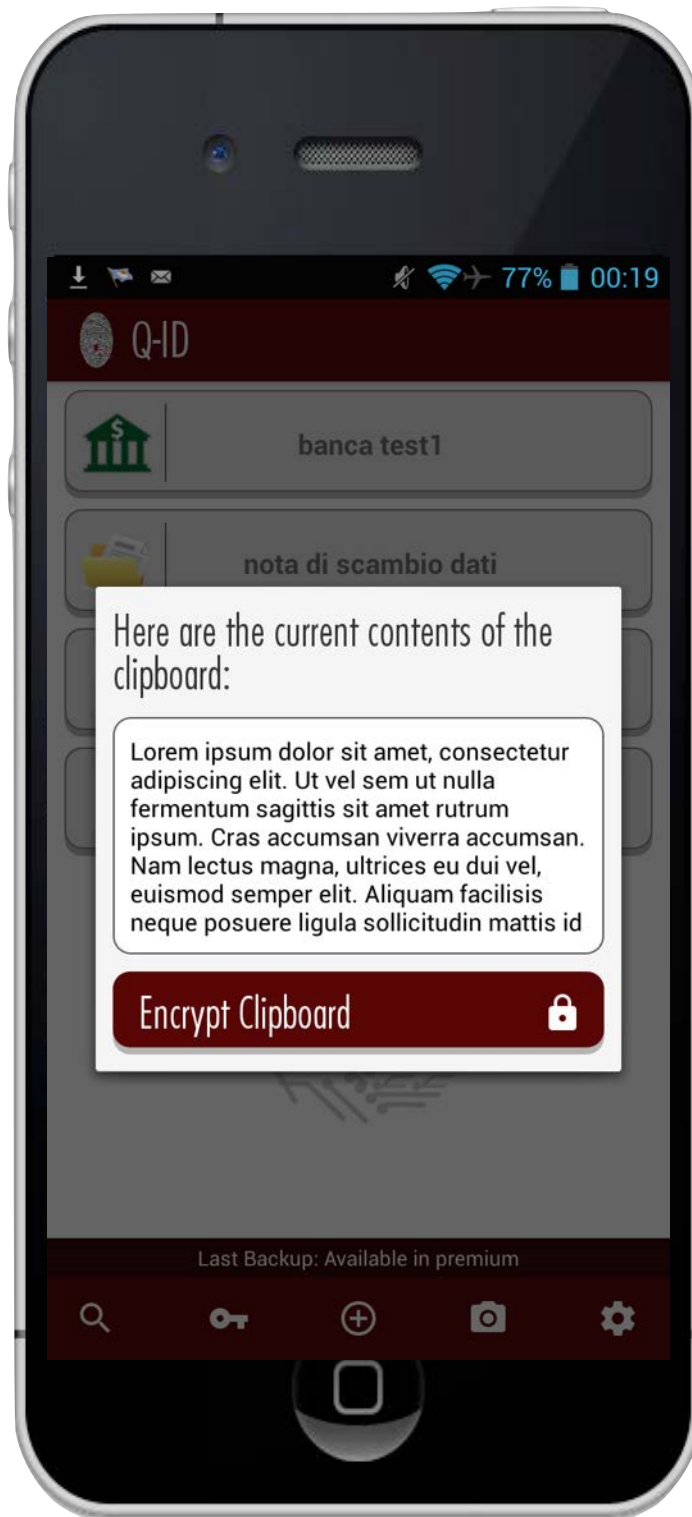
visualizza / nascondi
i dati dei campi password e pin

aggiungi Tag
specifici o condivisi
per la Card

salva la Card corrente

cancella il contenuto di
tutti i campi della card

ulteriori funzioni



L'utente avrà la possibilità di codificare o decodificare un testo presente nella clipboard, digitando una password ovvero utilizzando una password presente all'interno di una delle schede.

In questo modo, sarà capace di gestire messaggi di testo per email, SMS, whatsUp o altre applicazioni presenti sullo smartphone; con assoluta sicurezza e privacy.

La funzione utilizza lo Standard Symmetric Code (AES); richiede che le parti, condividano la stessa chiave (sharedKey)

Un esempio di messaggio codificato (in stile GPG/PGP):

```
-----BEGIN Q-ID MESSAGE-----
```

```
Version: Q-ID 1.0.2 - www.q-id.com
```

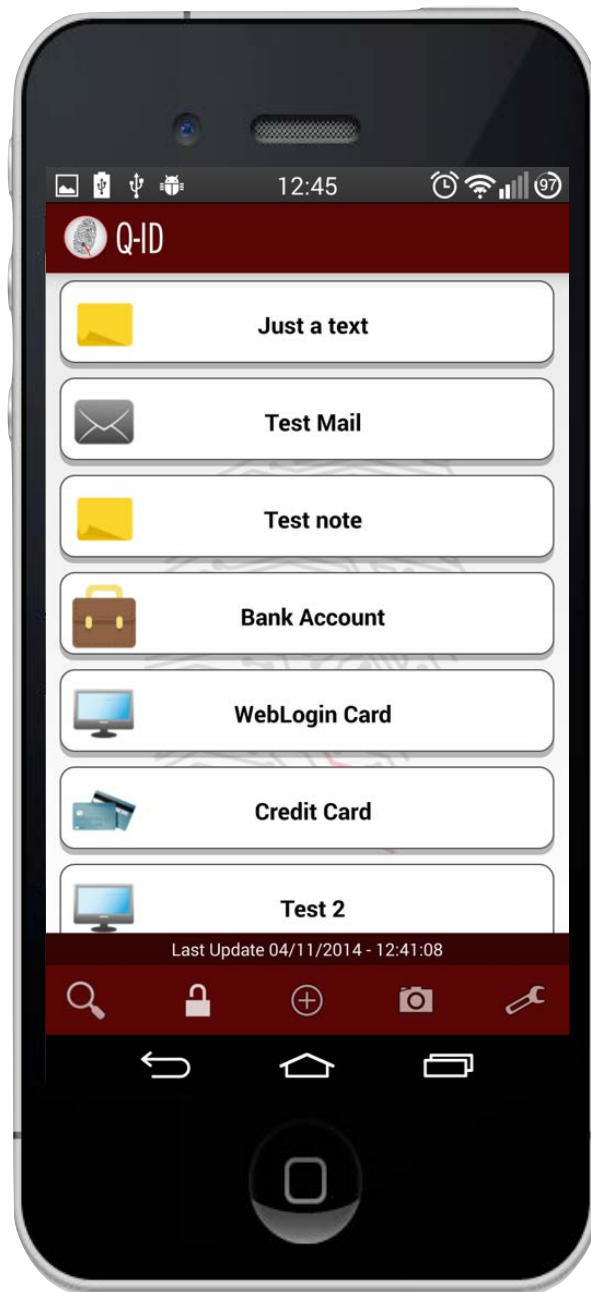
```
RDMFqhRWO5ahYyR8XNYhakKsLN3homjPMyQgM/GDFv1Xu47EIJrs/UVQM//3c9VA
M+BiSMmdu9KVSXkMLuPdXxQsidiDkE8Jb8DOh0SuhCeGZ/7u6IfYGseqqMqNICYq
7xPXFOPoP8+87SZVoAK+8UZWcYHAL/pddmJrR5Q//6cnbjuxm58iTqiKq1xJoNu9
S3QMI3FK0kcBADMQrk7WQY3wxzNRuGb+XBt08TZ+gI5SS9bSa4A9/2e7uo9bDLrG
B6h/JaAFEmq+BoYDcowJTZVAZTPxvcoMqSKOeyTEMg==
=beEb
```

```
-----END Q-ID MESSAGE-----
```

La funzione di codifica/decodifica di messaggi, è presente nella versione gratuita.

The Save&Restore function is valid for premium members only.

Selezionando "Sync", l'App Q-ID, effettua una richiesta di disponibilità al server centrale Q-ID, poi inizia a sincronizzare le schede tra smartphone e server.



Tutte le informazioni si muovono attraverso un canale sicuro (SSL), inoltre le informazioni sono codificate alla fonte sul cellulare.

L'utente è l'unico proprietario delle proprie informazioni.

NOTA: per ragioni di sicurezza e per security policy, a discrezione del fornitore, alcune schede OTP non saranno oggetto di backUp.

Questi specifici OTP, devono vivere su un'unica device.

L'Azienda Q-ID non ha nessuna conoscenza dei vostri dati.

Noi non conosciamo la vostra Master Password, ne vogliamo conoscerla.

L'unica cosa che sappiamo con sicurezza sui vostri dati, è rappresentata dal numero di schede che avete sincronizzato e quando lo avete fatto.

Sui nostri server, vediamo solo blocchi di dati codificati — non le vostre userID, PIN, password e neppure semplici note che possiate aver scritto in una scheda: **we have zero knowledge on your data.**