mobysign_

yes it's me

Soluzioni di autenticazione SPID
LIVELLO 2 e 3

ITside Srl
Via S. da Corbetta, 29/A
20011 Corbetta (MI)

Mobysign Limited
222, Regent Street, London

Tecnologia

- **una chiave privata** archiviata in una memoria sicura nello smartphone e protetta da un **PIN**

- architettura client-server

Lo smartphone, strumento di autenticazione per transazioni originate

-sullo stesso smartphone

-da altri device, come il PC

Autenticazione

1. **La app di autenticazione è installata su un device mobile di tipo smartphone e si connette ad una una architettura server**
2. **La app è disponibile al download direttamente dal device con collegamento diretto al relativo *marketplace* ufficiale Android/Apple/RIM/Microsoft o a *marketplace* privativo riconosciuto dall'identity provider**
3. **Il codice (sorgente o) eseguibile della app è firmato dal *vendor*, quale l'identity provider o suo fornitore tecnologico di autenticazione, secondo i meccanismi adottati dal marketplace in modo che la app sia esplicitamente riconducibile al vendor da parte dell'utente finale**
4. **Il sistema operativo del device prevede una *area sicura della app* come un'area persistente di memoria riservata in modo esclusivo alla app**
5. **il device non deve essere jailbreaked o rooted**
6. **la chiave privata di firma PKI di 1024 bit o superiore è generata e conservata a bordo di una *memoria sicura* quale:**
   a) **una microSD o secure element embedded (o processore) certificati CCEAL4+ e connessi fisicamente al dispositivo**
   b) **una memoria sicura come nel caso a) con certificazioni meno stringenti o FIPS oppure l'area sicura della app**

Autenticazione

7. Con digitazione del PIN da parte dell'utente, viene eseguita una firma PKI su un testo unico e variabile ad ogni richiesta di autenticazione e viene inviata la firma al server
8. La architettura server effettua la verifica della firma PKI
9. Ogni comunicazione device-server è cifrata e utilizza il canale https
10. Dopo l'inserimento di un numero configurabile di PIN errati il server non abilita le richieste di autenticazione
11. La richiesta di autenticazione avviene su un mezzo di elaborazione, distinto dal device o coincidente con esso, dove l'utente digita o fa pervenire con mezzi di prossimità (QR code etc..) il proprio username (o nickname scelto dall'utente durante la registrazione o numero di telefono se presente in registrazione) e visualizza gli estremi della transazione di richiesta di autenticazione ed inoltre tali informazioni sono visualizzate anche sul device di autenticazione (doppio canale)
12. La richiesta di autenticazione si presenta sul dispositivo sotto forma di popup che riporta il testo da firmare con digitazione PIN via tastiera touch integrata o fisica
13. Il popup viene inviato attraverso i sistemi push messi a disposizione dal sistema operativo e/o attraverso altri sistemi di identificazione del device

mobysign
yes it's me

Identificazione

1. **Identificazione de visu, o via webcam, via bonifico, via e/m banking da parte dell'utente finale, o via richiesta di emissione di una carta di credito/bancomat/debito da parte dell'utente finale o apertura conto corrente secondo le procedure definite dal soggetto finanziario che eroga il servizio, compliant con Banca d'Italia e le raccomandazioni della BCE.**
2. **In caso di bonifico, verifica che l'identificativo fornito all'utente sia presente nella causale del bonifico effettivamente eseguito**
3. **A seguito della identificazione il soggetto identificatore rilascia uno username (eventualmente lo stesso dell'e/m banking) e un Activation Code, e popola con i dati utente una Registration Authority legata all'Identity Provider**
4. **L'utente effettua la registrazione sulla app scegliendo nella procedura l'identity provider e digitando username e activation code per verifica**
5. **Viene generata su memoria sicura una coppia di chiavi richiedendo all'utente di scegliere il relativo PIN**
6. **Viene effettuata una richiesta di certificato con gli schemi classici**