

Tesi di Laurea Magistrale in Secure Systems Design

***Progettazione e Sviluppo di un Modulo Software per
Smart Card Contactless NFC su Dispositivi Android***

Anno Accademico 2017/2018

relatori

Ch.ma Prof. Valentina Casola

Ch.mo Prof. Nicola Mazzocca

Ch.mo Prof. Porfirio Tramontana

relatore aziendale

Ing. Vincenzo Terracciano

candidato

Pasquale Angelino

Matr. M63000416

L'identità digitale in Italia

- L'**identità digitale** è la rappresentazione virtuale di un soggetto reale nelle sue interazioni coi sistemi informatici, in particolare per l'accesso a servizi digitalizzati pubblici e privati.
- Il suo percorso nel nostro Paese è stato oggetto di innumerevoli controversie amministrative e politiche, che hanno originato i seguenti strumenti di identificazione, attualmente coesistenti:

- ◆ Username/Password
- ◆ Personal Identification Number (PIN)
- ◆ Carta Nazionale dei Servizi (CNS)
- ◆ Tessera Sanitaria - CNS (TS-CNS)
- ◆ **Carta d'Identità Elettronica (CIE)**



La Carta d'Identità Elettronica - CIE 3.0

- La **CIE**, oltre ad essere un documento fisico che attesta l'identità del titolare, rappresenta uno strumento pensato per realizzare un gran numero di opportunità “digitali” per il cittadino, fra le quali l'*autenticazione* sui diversi portali web offerti dalle Pubbliche Amministrazioni.



Attuali soluzioni di autenticazione con CIE

- Il **Software CIE** (c.d. “Middleware”) realizza l’accesso da desktop ai servizi on-line disponibili per l’utente, ma implica l’impiego da parte dello stesso di un *lettore di tipo contactless* per la comunicazione sicura con la smart card.
- In Germania sono già state proposte soluzioni che consentono all’utente di servirsi di un dispositivo per lui più comodo ed immediato, ossia un comune **smartphone con supporto NFC**.

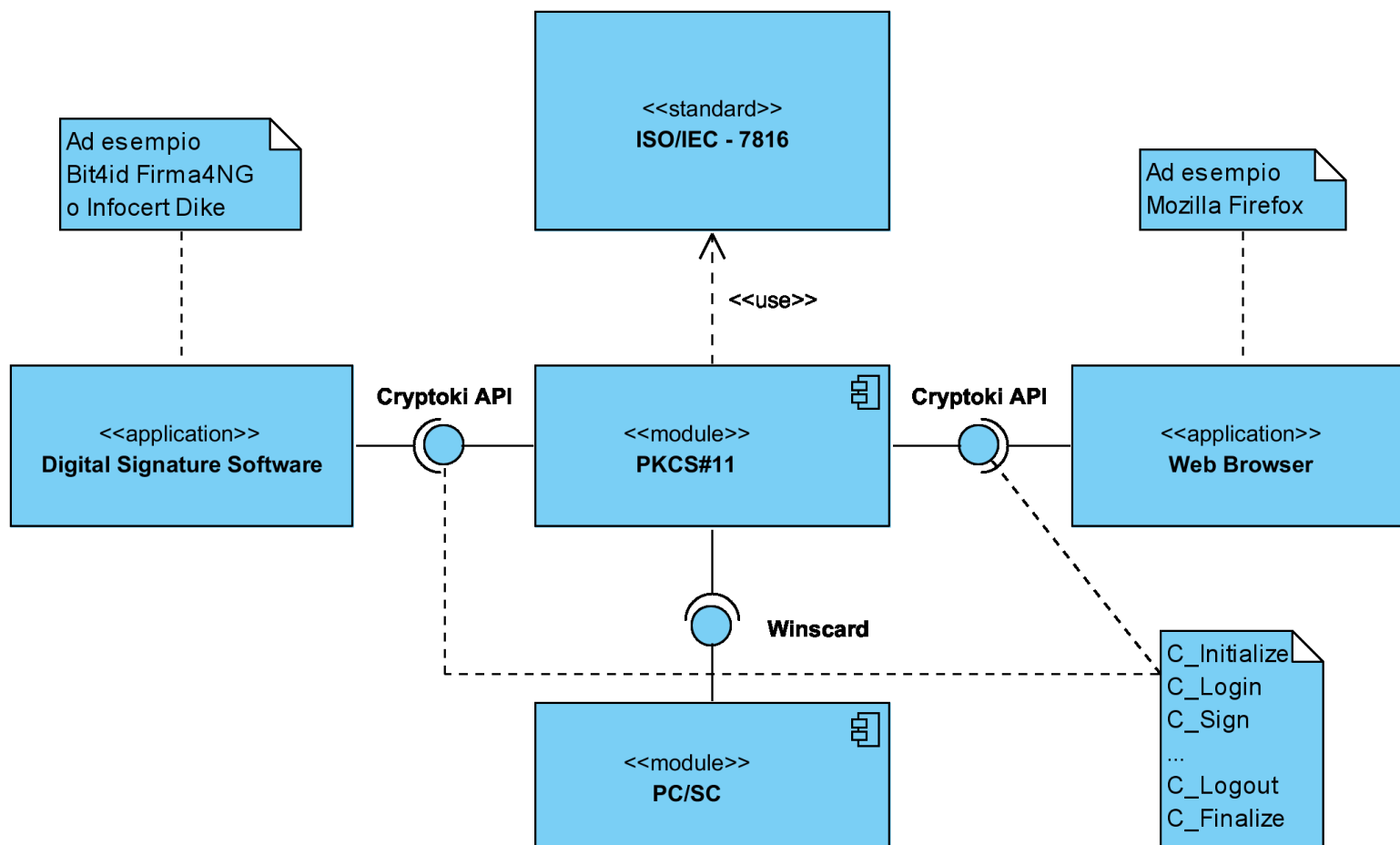


F-Droid

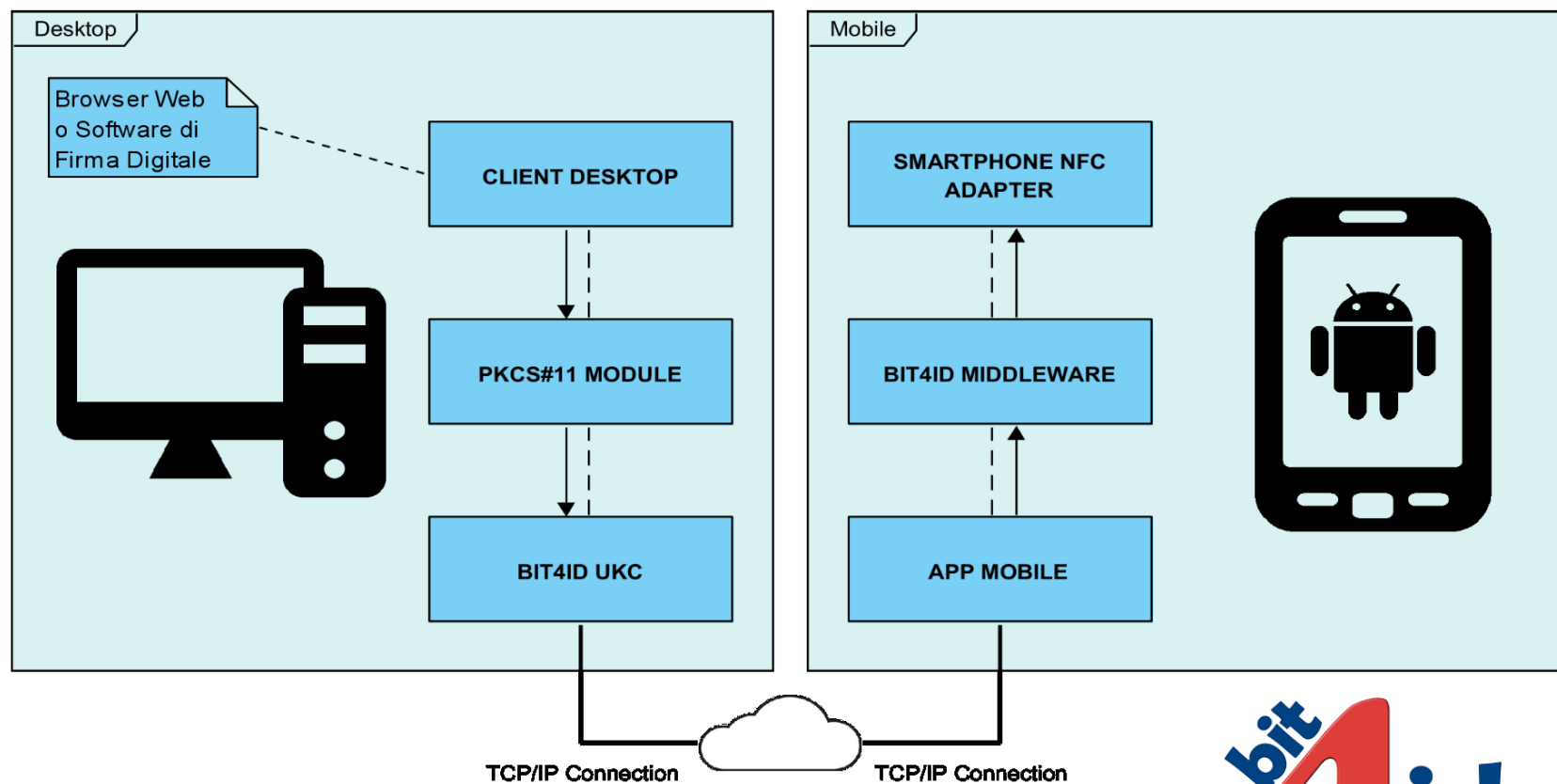


AusweisApp 2

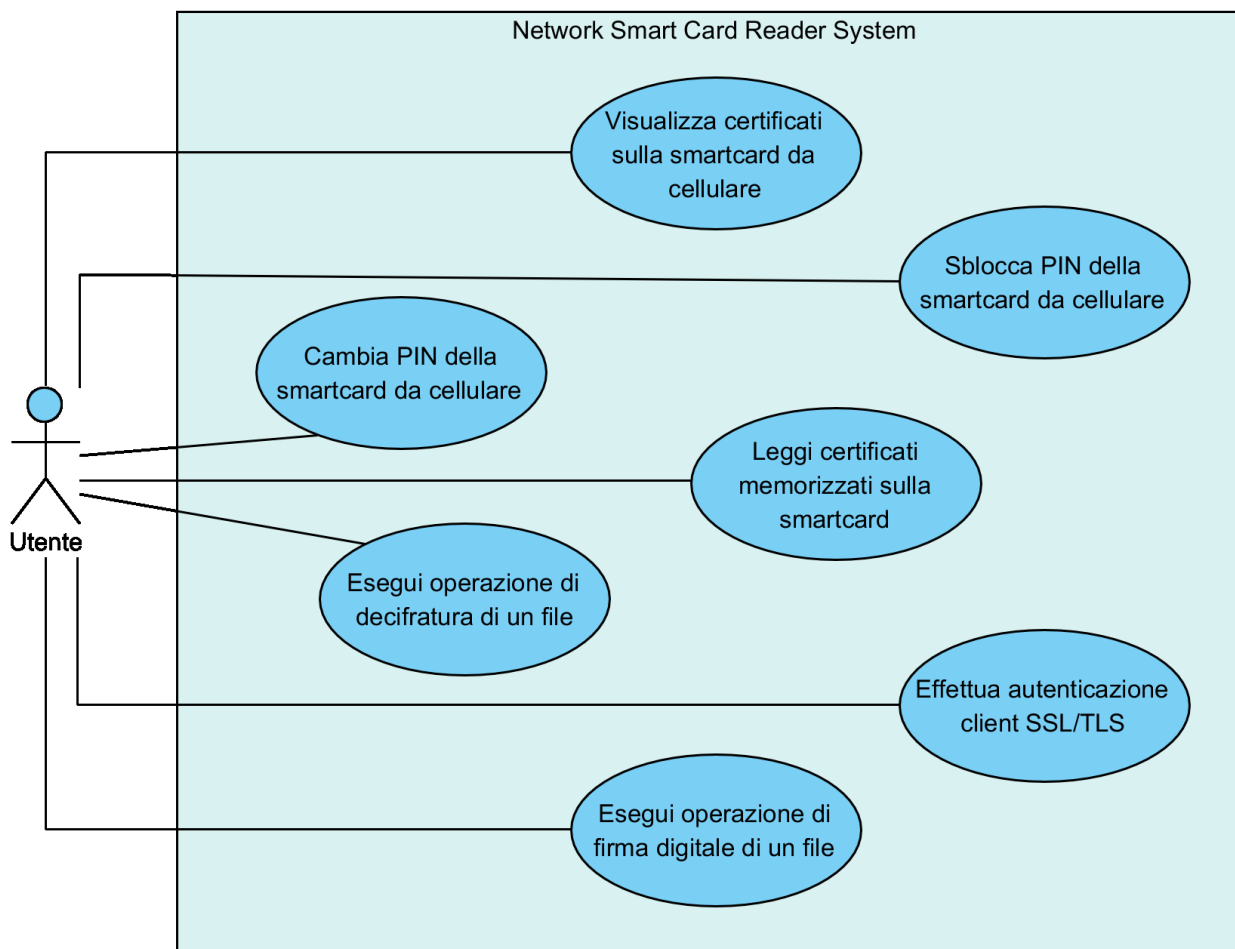
Arch. di sistema tradizionale con PKCS#11



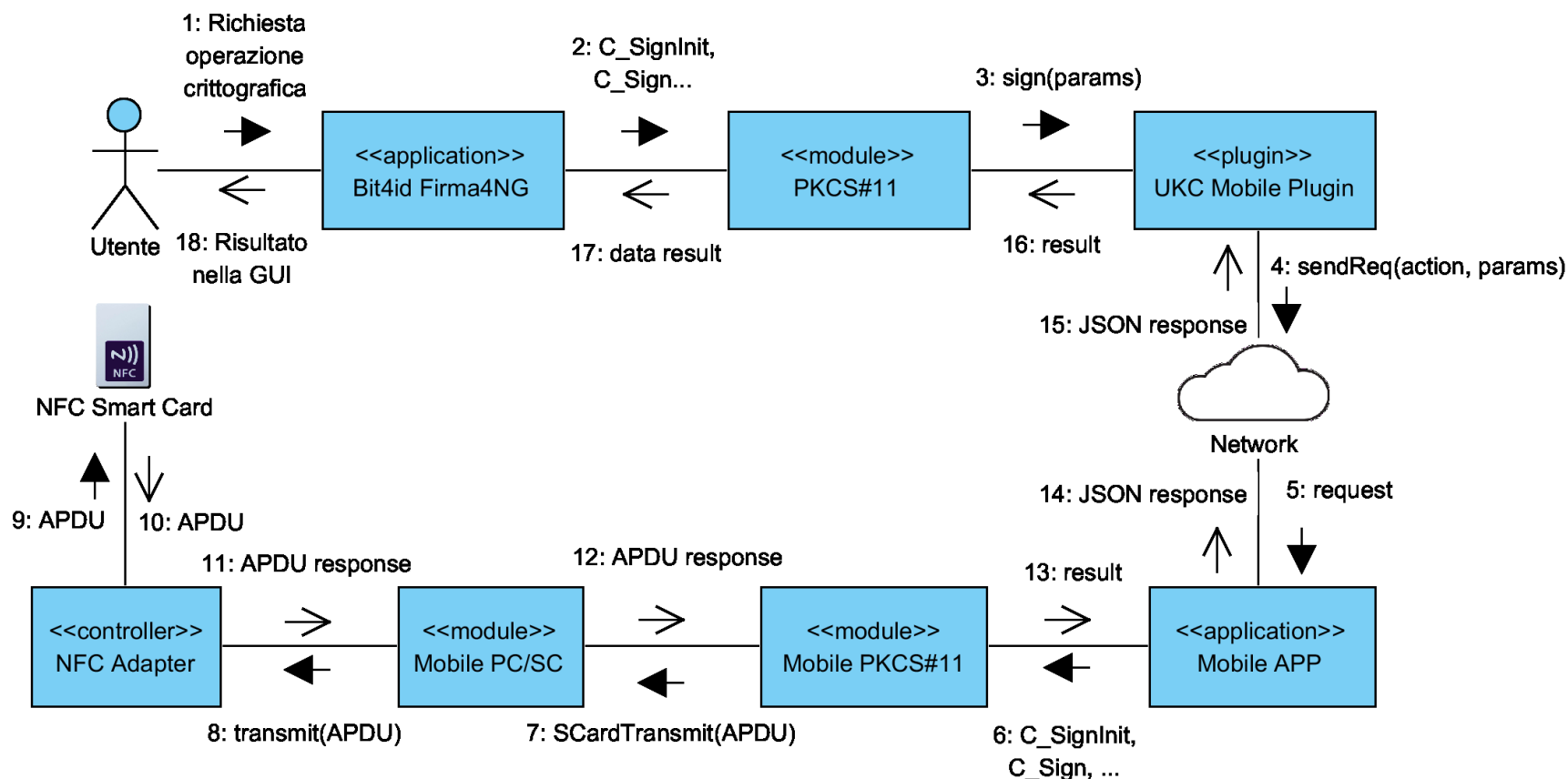
Soluzione proposta



Casi d'uso del sistema

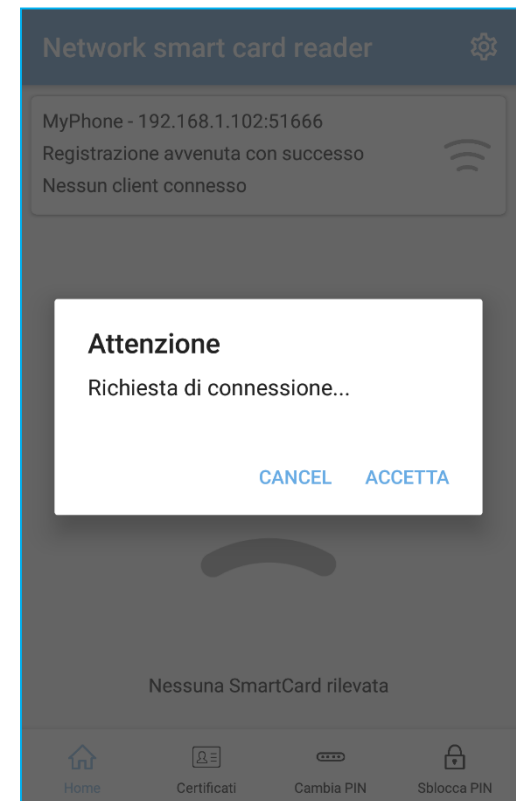
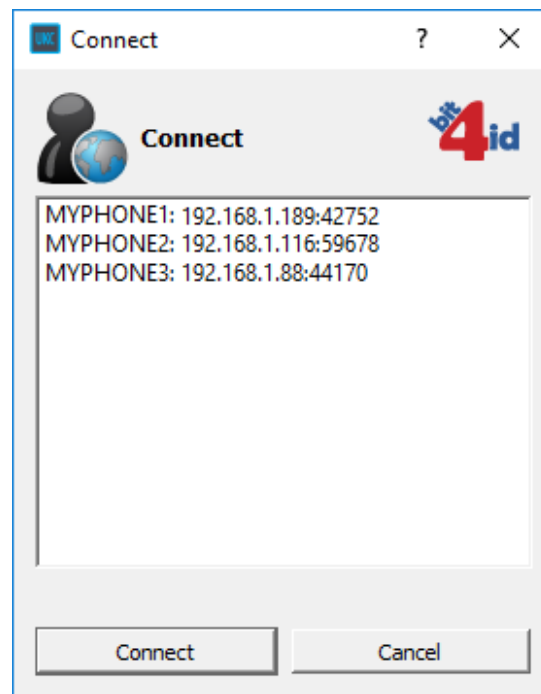
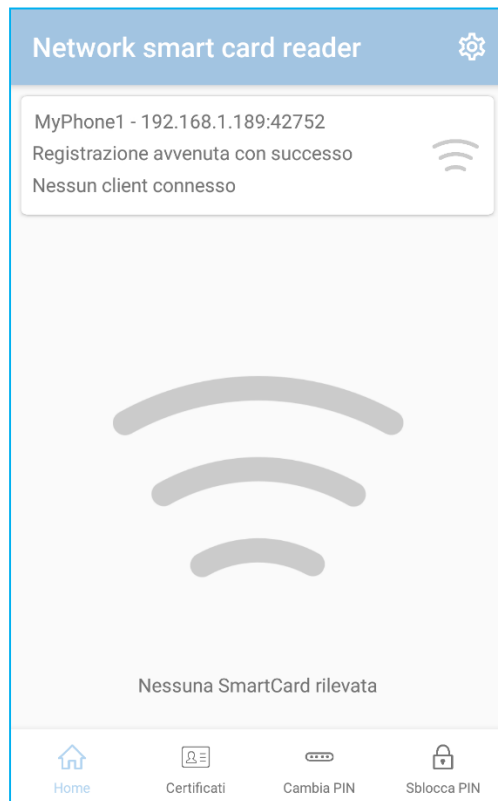


Flusso di comunicazione desktop/mobile



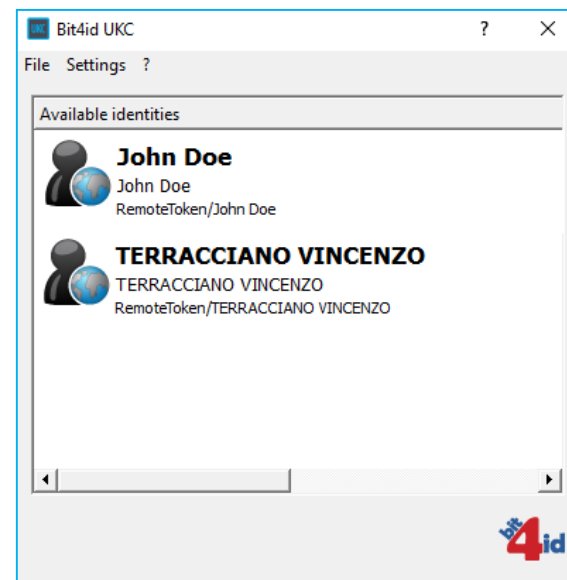
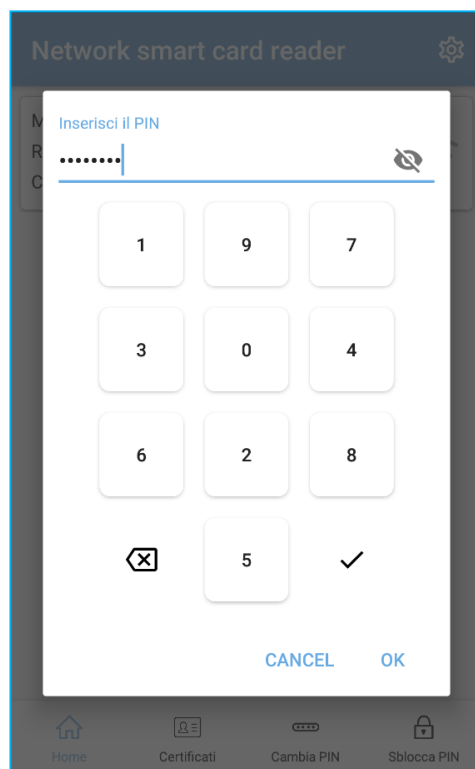
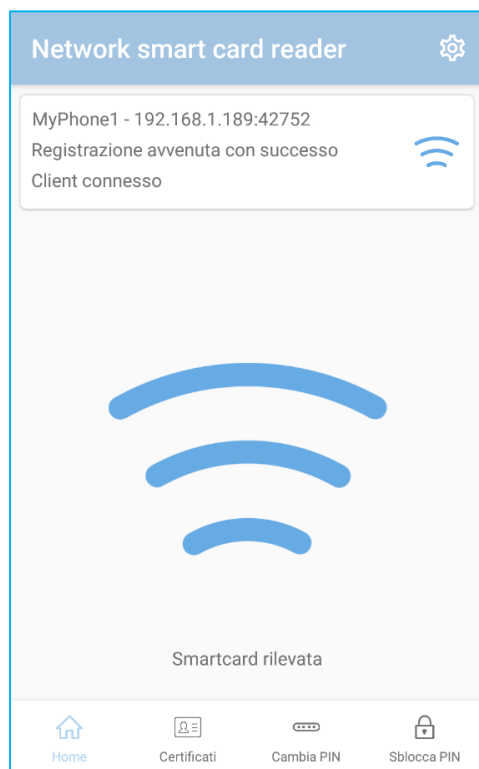
Registrazione e connessione al lettore di rete

- Il lettore di rete viene annunciato con l'impiego del protocollo **Zeroconf**.

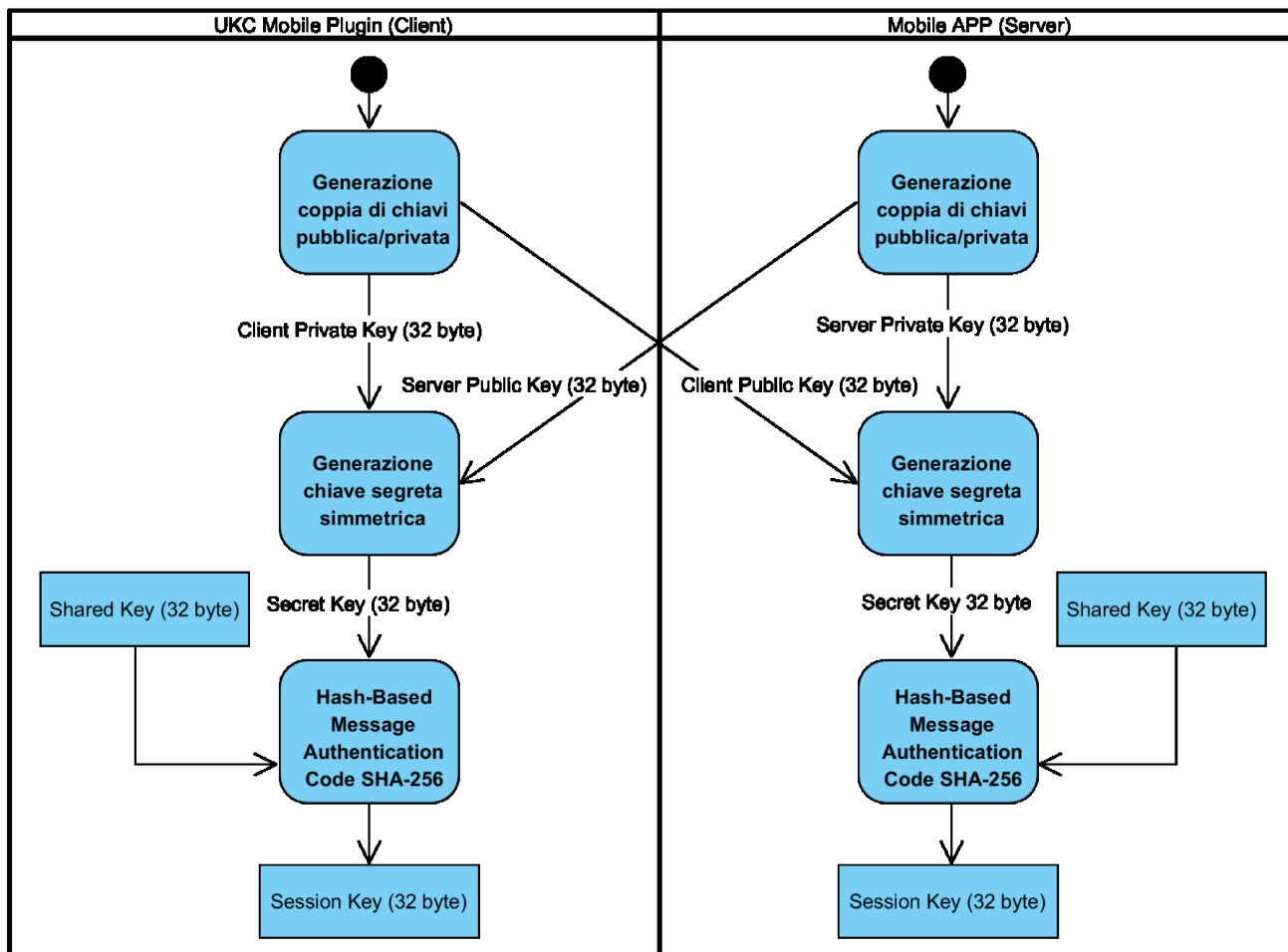


Connessione avvenuta e caricamento certificati

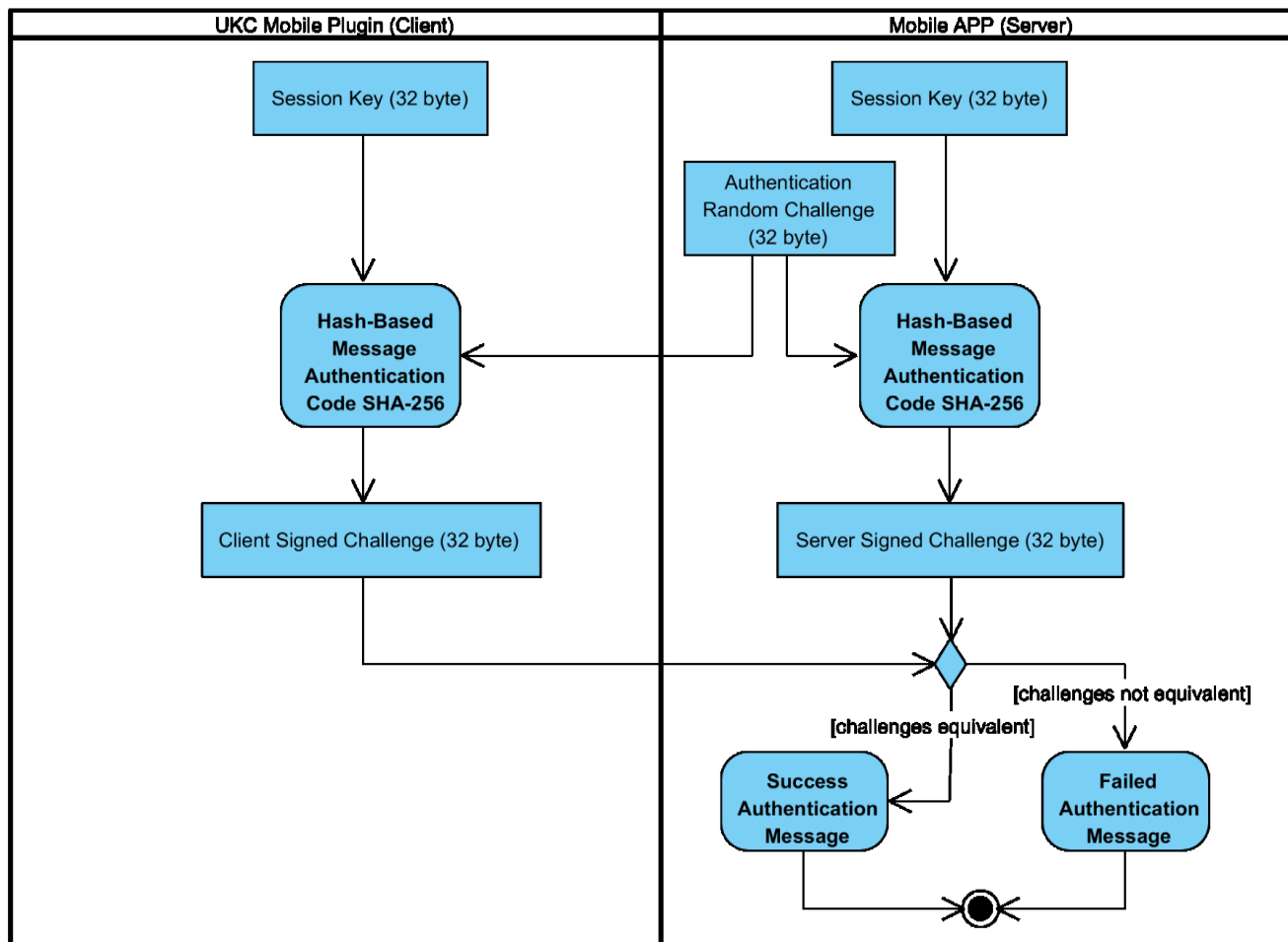
- Il PIN della carta *viene inserito lato mobile* per evitarne la trasmissione.



Schema di autenticazione e cifratura (1/2)

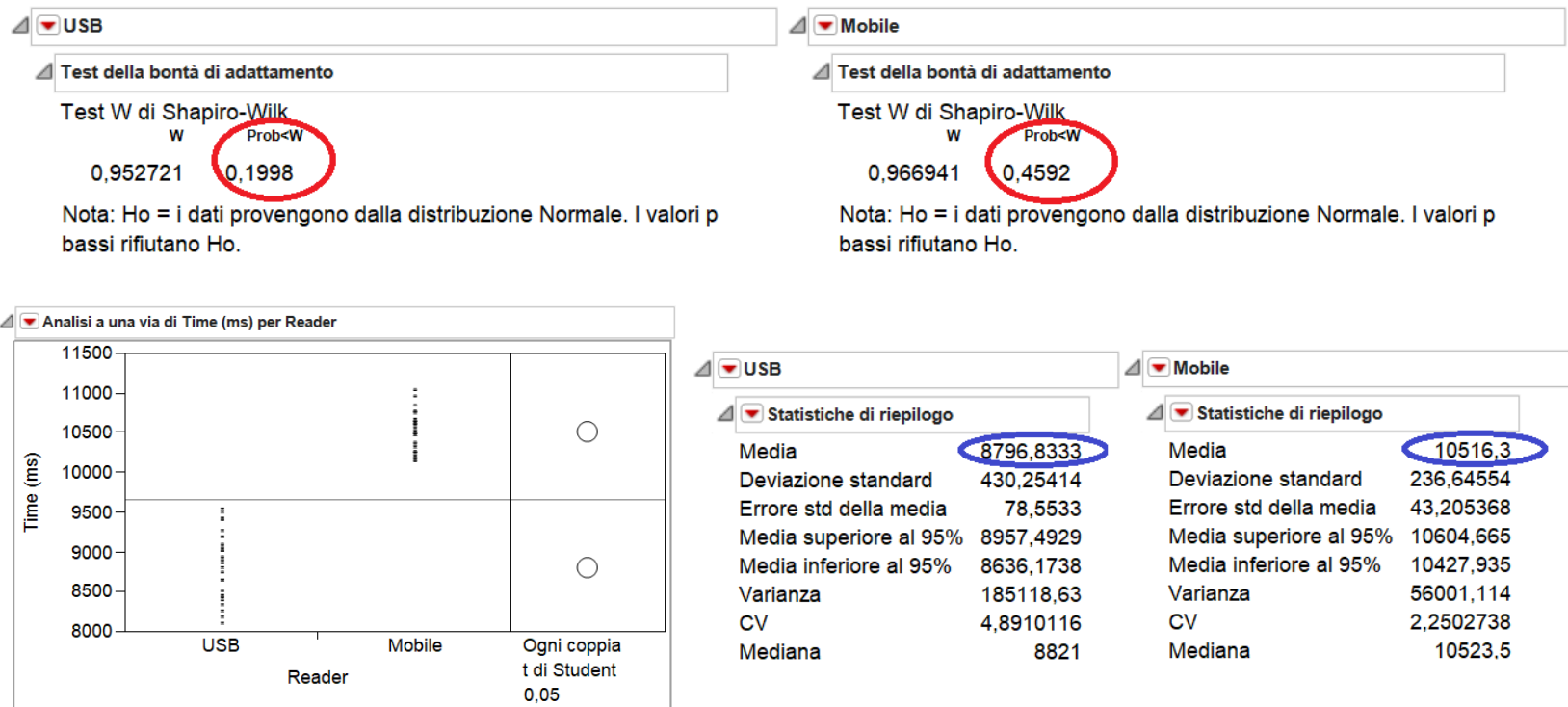


Schema di autenticazione e cifratura (2/2)



Confronto con lettore USB di smartcard NFC

- Sono state effettuate 30 misurazioni per *confrontare i tempi di risposta*, per un'operazione di firma, con un lettore da tavolo e quello di rete ideato.



Risultati e conclusioni

- Con questo lavoro si è raggiunto l'obiettivo di offrire all'utente la possibilità di svincolarsi dall'acquisto di un lettore contactless di smartcard ed utilizzare al suo posto il proprio smartphone con supporto NFC.
- Sono stati condotti una serie di *test funzionali e di integrazione* fra le componenti del sistema, per diversi sistemi operativi e configurazioni software, che hanno tutti dato prova dell'efficacia della soluzione realizzata.
- Le misurazioni effettuate hanno evidenziato la validità della soluzione proposta anche dal punto di vista prestazionale, con uno scarto in media di soli 1.7 secondi rispetto ad un lettore da tavolo USB di smartcard NFC.
- L'applicazione è predisposta all'aggiunta nella schermata principale di una funzionalità che consenta di verificare l'esattezza dei dati anagrafici (*MRTD*) a bordo del microprocessore della Carta di Identità Elettronica.
- Potrà, infine, essere integrato un *browser* nell'APP per effettuare anche da mobile, durante la navigazione, operazioni di client authentication SSL/TLS.

Grazie per la vostra attenzione!