Ministero dello Sviluppo Economico

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

OCSI

Organismo di Certificazione della Sicurezza Informatica

Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti ICT
(DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)

Certificato n. 2/16

(Certification No.)

Prodotto: **IDentity Card v3.2/PACE-EAC1**
(Product)

Sviluppato da: **ID&Trust**
(Developed by)

Il prodotto indicato in questo certificato è risultato conforme ai requisiti dello standard ISO/IEC 15408 (Common Criteria) v. 3.1 per il livello di garanzia:

The product identified in this certificate complies with the requirements of the standard ISO/IEC 15408 (Common Criteria) v. 3.1 for the assurance level:

EAL4+
(ALC_DVS.2, ATE_DPT.2, AVA_VAN.5)

Il Direttore
(Dott.ssa Rita Forsi)

Roma, 22 marzo 2016

Common Criteria

SOGIS
IT SECURITY CERTIFIED

Questa pagina è lasciata intenzionalmente vuota

Ministero dello Sviluppo Economico

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Rapporto di Certificazione

IDentity Card v3.2/PACE-EAC1

OCSI/CERT/SYS/02/2016/RC

Versione 1.0

22 marzo 2016

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	OCSI	Prima emissione	22/03/2016

2 Indice

3 Elenco degli acronimi

BAC Basic Access Control

CC Common Criteria

CCRA Common Criteria Recognition Arrangement

CEM Common Evaluation Methodology

DPCM Decreto del Presidente del Consiglio dei Ministri

EAL Evaluation Assurance Level

eMRTD electronic Machine Readable Travel Document

HW Hardware

LGP Linea Guida Provvisoria

LVS Laboratorio per la Valutazione della Sicurezza

NIS Nota Informativa dello Schema

OCSI Organismo di Certificazione della Sicurezza Informatica

ODV Oggetto della Valutazione

PACE Password Authenticated Connection Establishment

PP Profilo di Protezione

RFV Rapporto Finale di Valutazione

SAR Security Assurance Requirement

SFR Security Functional Requirement

SW Software

TDS Traguardo di Sicurezza

TOE Target of Evaluation

TSF TOE Security Functionality

TSFI TOE Security Functionality Interface

4 Riferimenti

[CC1] CCMB-2012-09-001, “Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model”, Version 3.1, Revision 4, September 2012

[CC2] CCMB-2012-09-002, “Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components”, Version 3.1, Revision 4, September 2012

[CC3] CCMB-2012-09-003, “Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance components”, Version 3.1, Revision 4, September 2012

[CCRA] “Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security”, July 2014

[CCRA-2000] “Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security”, May 2000

[CEM] CCMB-2012-09-004, “Common Methodology for Information Technology Security Evaluation – Evaluation methodology”, Version 3.1, Revision 4, September 2012

[LGP1] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Descrizione Generale dello Schema Nazionale - Linee Guida Provvisorie - parte 1 – LGP1 versione 1.0, Dicembre 2004

[LGP2] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Accreditamento degli LVS e abilitazione degli Assistenti - Linee Guida Provvisorie - parte 2 – LGP2 versione 1.0, Dicembre 2004

[LGP3] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Procedure di valutazione - Linee Guida Provvisorie - parte 3 – LGP3, versione 1.0, Dicembre 2004

[NIS1] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 1/13 – Modifiche alla LGP1, versione 1.0, Novembre 2013

[NIS2] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 2/13 – Modifiche alla LGP2, versione 1.0, Novembre 2013

[NIS3] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 3/13 – Modifiche alla LGP3, versione 1.0, Novembre 2013

[SOGIS] “Mutual Recognition Agreement of Information Technology Security Evaluation Certificates”, Version 3, January 2010

[ADM] IDentity Applet Administrator's Guide Version 3.2.18

[AFNOR-1] AFNOR BSI contribution to TF4 Amendment to ICAO Technical Report – RF protocol and application test standard for ePassport Part 3, Tests for Application Protocol and Logical Data Structure, Version 1.01, February 2007 Supplemental Access Control Active Authentication

[AFNOR-2] AFNOR Advanced Security Mechanisms For Machine Readable Travel Documents – Extended Access Control (EAC) Tests For Security Implementation V.1.12, October 3, 2008

[BSI-56] BSI-CC-PP-0056-V2-2012, Machine Readable Travel Document with "ICAO Application", Extended Access Control with PACE, Version 1.3

[BSI-68] BSI-CC-PP-0068-V2-2011, Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE_PP), Version 1.0

[CCDB] CCDB-2012-04-001, Supporting Document, Mandatory Technical Document, Composite product evaluation for Smart Cards and similar devices, Version 1.2, April 2012

[CHANGES] CC Re-evaluation eMRTD with BAC, PACE-EAC1, "Changes of ID&Trust Identity Card 3.1 to 3.2", ID&Trust, Version 0.1, 25 October 2015

[CONF] IDentity Applet Initialization and configuration Version 3.2.07

[ETR-COMP] ETR for Composite Evaluation NXP J3E145_M64, J3E120_M65, J3E082_M65, J2E145_M64, J2E120_M65, and J2E082_M65 Secure Smart Card Controller Revision 3 EAL5+, Brightsight, 9 August 2013, revision 12 August 2014

[IAR] Impact Analysis Report "Changes of ID&Trust IDentity Card 3.1 to 3.2", Systrans SW Lab, Version 1.3, 13 November 2015

[ICAO-RF] ICAO RF protocol and application test standard for e-passport - part 3 v.2.01

[ICAO-TR] International Civil Aviation Organization, ICAO Machine Readable Travel Documents, Technical Report, Supplemental Access Control for Machine Readable Travel Documents, Version 1.00, November 2010

[ICAO-9303] International Civil Aviation Organization, ICAO Doc 9303, Machine Readable Travel Documents, part 1 – Machine Readable Passports, Sixth Edition, 2006

[NSCIB] Certification Report "NXP J3E145_M64, J3E120_M65, J3E082_M65, J2E145_M64, J2E120_M65, and J2E082_M65 Secure Smart Card Controller Revision 3", NSCIB-CC-13-37760-CR2, 5 August 2013, revision 26 August 2014

[RC] Rapporto di Certificazione, "ID&Trust IDentity Card v3.1/PACE-EAC1", OCSI/CERT/SYS/04/2015/RC, versione 1.0, 30 settembre 2015

[RFV] ID&Trust IDentity Card v3.2/PACE-EAC1 Evaluation Technical Report, v1.1, 8 March 2016

[TDS] ID&Trust IDentity Card v3.2/PACE-EAC1 Security Target, v0.43, 8 March 2016

[TR-210] BSI Technical Guideline TR-03110-1, Advanced Security Mechanisms for Machine Readable Travel Documents – Part 1 – eMRTDs with BAC/PACEv2 and EACv1, Version 2.10, 20 March 2012

[TR-220] BSI Technical Guideline TR-03110-4 – Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 4 – Applications and Document Profiles, Version 2.20, 3 February 2015

[USR] IDentity Applet User's Guide Version 3.2.19

5 Riconoscimento del certificato

5.1 Riconoscimento di certificati CC in ambito europeo (SOGIS-MRA)

L'accordo di mutuo riconoscimento in ambito europeo (SOGIS-MRA, versione 3, [SOGIS]) è entrato in vigore nel mese di aprile 2010 e prevede il riconoscimento reciproco dei certificati rilasciati in base ai Common Criteria (CC) per livelli di valutazione fino a EAL4 incluso per tutti i prodotti IT. Per i soli prodotti relativi a specifici domini tecnici è previsto il riconoscimento anche per livelli di valutazione superiori a EAL4.

L'elenco aggiornato delle nazioni firmatarie e dei domini tecnici per i quali si applica il riconoscimento più elevato e altri dettagli sono disponibili su http://www.sogisportal.eu.

Il logo SOGIS-MRA stampato sul certificato indica che è riconosciuto dai paesi firmatari secondo i termini dell'accordo.

Il presente certificato è riconosciuto in ambito SOGIS-MRA fino a EAL4.

5.2 Riconoscimento di certificati CC in ambito internazionale (CCRA)

La nuova versione dell'accordo internazionale di mutuo riconoscimento dei certificati rilasciati in base ai CC (Common Criteria Recognition Arrangement, [CCRA]) è stata ratificata l'8 settembre 2014. Si applica ai certificati CC conformi ai Profili di Protezione "collaborativi" (cPP), previsti fino al livello EAL4, o ai certificati basati su componenti di garanzia fino al livello EAL 2, con l'eventuale aggiunta della famiglia Flaw Remediation (ALC_FLR).

I certificati rilasciati prima dell'8 settembre 2014 sono ancora riconosciuti secondo le regole del precedente accordo [CCRA-2000], cioè fino al livello EAL 4 (e ALC_FLR). Queste stesse regole del CCRA-2000 si applicano ai processi di certificazione in corso alla data dell'8 settembre 2014, come pure al mantenimento e alla ri-certificazione di vecchi certificati, per un periodo di transizione fino all'8 settembre 2017.

L'elenco aggiornato delle nazioni firmatarie e dei Profili di Protezione "collaborativi" (cPP) e altri dettagli sono disponibili su http://www.commoncriteriaportal.org.

Il logo CCRA stampato sul certificato indica che è riconosciuto dai paesi firmatari secondo i termini dell'accordo.

Poiché questo processo è la ri-certificazione di una precedente versione dello stesso prodotto, il presente certificato è riconosciuto secondo le regole del precedente accordo [CCRA-2000], cioè fino a EAL 4.

6 Dichiarazione di certificazione

L'oggetto della valutazione (ODV) è il prodotto "ID&Trust ID Card 3.2: NXP JCOP 2.4.2 R3 Smart Card with ID&Trust IDentity Applet Suite 3.2/PACE-EAC1", nome abbreviato "IDentity Card v3.2/PACE-EAC1", sviluppato dalla società ID&Trust.

L'ODV è un prodotto composito e comprende:

- la Piattaforma "NXP J3E120_M65 / J2E120_M65 / J3E082_M65 / J2E082_M65 Secure Smart Card Controller Revision 3", nome abbreviato "JCOP 2.4.2 R3", già certificata CC a livello EAL5 con aggiunta di ASE_TSS.2, ALC_DVS.2 e AVA_VAN.5 [NSCIB];
- la parte applicativa dell'ODV "ID&Trust IDentity Applet Suite Version 3.2, configurata come applicazione eMRTD;
- la documentazione operativa associata.

Pertanto, la valutazione è stata eseguita utilizzando i risultati della certificazione CC della Piattaforma [NSCIB] e seguendo le raccomandazioni contenute nel documento "Composite product evaluation for Smart Cards and similar devices" [CCDB], come richiesto dagli accordi internazionali CCRA e SOGIS.

La valutazione è stata condotta in accordo ai requisiti stabiliti dallo Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione ed espressi nelle Linee Guida Provvisorie [LGP1, LGP2, LGP3] e nelle Note Informative dello Schema [NIS1, NIS2, NIS3]. Lo Schema è gestito dall'Organismo di Certificazione della Sicurezza Informatica, istituito con il DPCM del 30 ottobre 2003 (G.U. n.98 del 27 aprile 2004).

Il presente Rapporto di Certificazione è stato emesso a conclusione della ri-certificazione di una precedente versione dello stesso ODV (IDentity Card v3.1/PACE-EAC1), già certificato dall'OCSI (Certificato n. 2/15 del 30 settembre 2015 [RC]).

L'ODV può essere configurato e utilizzato per diversi tipi di prodotti d'identità elettronica in base allo standard BSI TR-03110, v2.10 [TR-210].

Nel frattempo, è stata rilasciata una nuova versione dello standard (BSI TR-03110, v2.20 [TR-220]), in cui sono state normalizzate molte caratteristiche precedentemente considerate opzionali. Una di queste consente il controllo di accesso per i gruppi di dati all'interno di certificati verificabili, le cosiddette "Estensioni di autorizzazione per attributi generici locali" (cfr. [TR-220] par. 2.2). Questa funzionalità è implementata dalla nuova versione del prodotto, ma non influenza le funzioni già certificate dell'ODV. Al fine di distinguere le due versioni, l'ODV viene rinominato "IDentity Card v3.2/PACE-EAC1".

Le modifiche effettuate sono state descritte dal Fornitore ID&Trust nel documento [CHANGES].

Si noti che le modifiche effettuate hanno comportato anche la revisione del Traguardo di Sicurezza [TDS]. Gli utenti dell'ODV sono quindi invitati a prendere visione anche del nuovo TDS.

Per verificare l'effettivo impatto delle modifiche, si è ritenuto necessario procedere a una ri-certificazione dell'ODV.

L'LVS Systrans SW Lab ha innanzitutto effettuato un'analisi di impatto delle differenze rispetto alla versione già certificata (IDentity Card v3.1/PACE-EAC1), riassumendone i risultati nel documento [IAR]. Su questa base, i valutatori hanno potuto quindi riutilizzare gran parte delle evidenze già fornite nella prima valutazione. In particolare, i test funzionali sono stati limitati all'esecuzione delle attività relative alle famiglie ATE_FUN.1 e ATE_IND.2, mentre non sono stati eseguiti nuovi test di intrusione.

Obiettivo della valutazione è fornire garanzia sull'efficacia dell'ODV nel rispettare quanto dichiarato nel Traguardo di Sicurezza [TDS], la cui lettura è consigliata ai potenziali acquirenti. Le attività relative al processo di valutazione sono state eseguite in accordo alla Parte 3 dei Common Criteria [CC3] e alla Common Evaluation Methodology [CEM].

L'ODV è risultato conforme ai requisiti della Parte 3 dei CC v 3.1 per il livello di garanzia EAL4, con aggiunta di ALC_DVS.2, ATE_DPT.2, AVA_VAN.5, in conformità a quanto riportato nel Traguardo di Sicurezza [TDS] e nella configurazione riportata in Appendice B di questo Rapporto di Certificazione.

La pubblicazione del Rapporto di Certificazione è la conferma che il processo di valutazione è stato condotto in modo conforme a quanto richiesto dai criteri di valutazione Common Criteria – ISO/IEC 15408 ([CC1], [CC2], [CC3]) e dalle procedure indicate dal Common Criteria Recognition Arrangement [CCRA] e che nessuna vulnerabilità sfruttabile è stata trovata. Tuttavia l'Organismo di Certificazione con tale documento non esprime alcun tipo di sostegno o promozione dell'ODV.

7 Riepilogo della valutazione

7.1 Introduzione

Questo Rapporto di Certificazione riassume l'esito della valutazione di sicurezza del prodotto "IDentity Card v3.2/PACE-EAC1" secondo i Common Criteria, ed è finalizzato a fornire indicazioni ai potenziali acquirenti per giudicare l'idoneità delle caratteristiche di sicurezza dell'ODV rispetto ai propri requisiti.

I potenziali acquirenti sono quindi tenuti a consultare il presente Rapporto di Certificazione congiuntamente al Traguardo di Sicurezza [TDS], che specifica i requisiti funzionali e di garanzia e l'ambiente di utilizzo previsto.

7.2 Identificazione sintetica della certificazione

Nome dell'ODV	IDentity Card v3.2/PACE-EAC1
Traguardo di Sicurezza	IDentity Card v3.2/PACE-EAC1 Security Target, v0.43, 8 marzo 2016
Livello di garanzia	EAL4 con aggiunta di ALC_DVS.2, ATE_DPT.2, AVA_VAN.5
Fornitore	ID&Trust
Committente	ID&Trust
LVS	Systrans SW Lab
Versione dei CC	3.1 Rev. 4
Conformità a PP	BSI-CC-PP-0056-V2-2012 [BSI-56], BSI-CC-PP-0068-V2-2011 [BSI-68]
Data di inizio della valutazione	24 febbraio 2016
Data di fine della valutazione	8 marzo 2016

I risultati della certificazione si applicano unicamente alla versione del prodotto indicata nel presente Rapporto di Certificazione e a condizione che siano rispettate le ipotesi sull'ambiente descritte nel Traguardo di Sicurezza [TDS].

7.3 Prodotto valutato

In questo paragrafo vengono sintetizzate le principali caratteristiche funzionali e di sicurezza dell'ODV; per una descrizione dettagliata, si rimanda al Traguardo di Sicurezza [TDS].

L'ODV "IDentity Card v3.2/PACE-EAC1" è un documento di viaggio elettronico costituito da una smart card con o senza contatto programmata in base ai requisiti e alle raccomandazioni definiti dall'International Civil Aviation Organization [ICAO-TR].

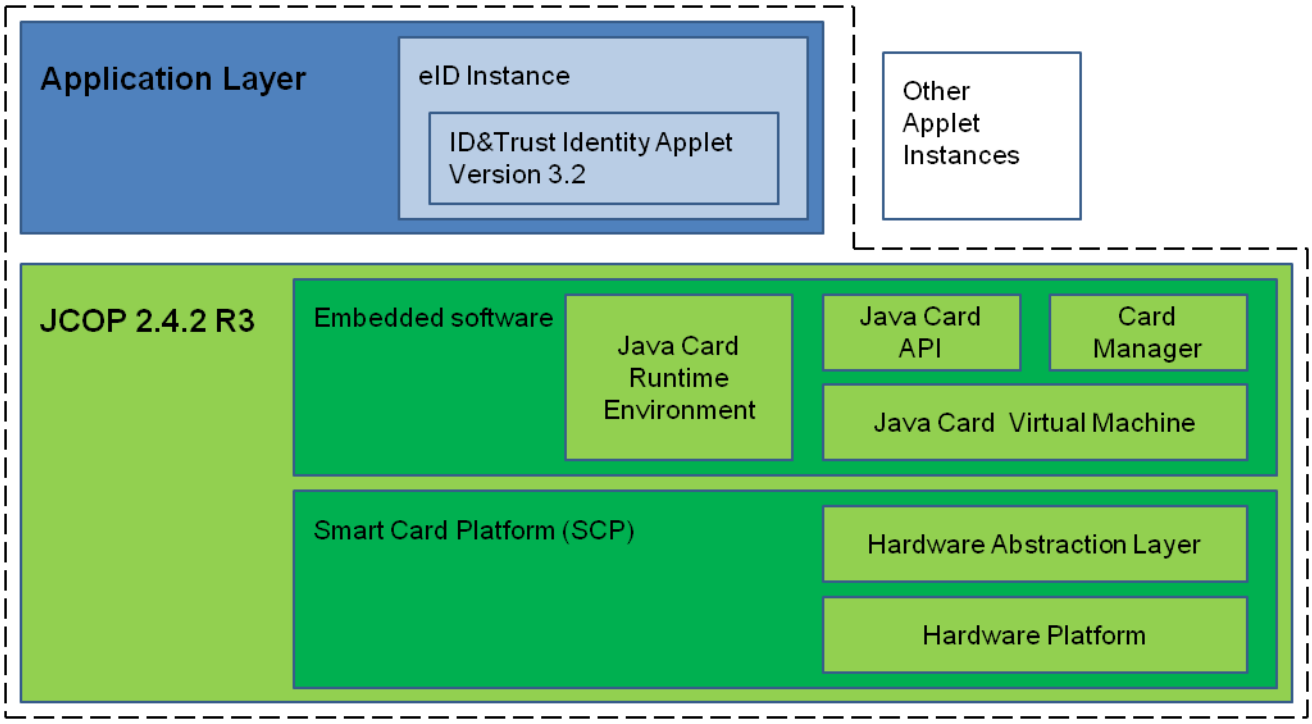

Figura 1 – L'architettura logica dell'ODV

L'ODV è un prodotto composito e comprende (Figura 1):

- la Piattaforma "NXP J3E120_M65 / J2E120_M65 / J3E082_M65 / J2E082_M65 Secure Smart Card Controller Revision 3", nome abbreviato "JCOP 2.4.2 R3", già certificata CC a livello EAL5 con aggiunta di ASE_TSS.2, ALC_DVS.2 e AVA_VAN.5 [NSCIB];
- la parte applicativa dell'ODV "ID&Trust IDentity Applet Suite Version 3.2", configurata come applicazione eMRTD;
- la documentazione operativa associata:
  - IDentity Applet Initialization and configuration Version 3.2.07 [CONF]
  - IDentity Applet Administrator's Guide Version 3.2.18 [ADM]
  - IDentity Applet User's Guide Version 3.2.19 [USR]

Il "cliente" dell'ODV è di solito l'Ente emettitore (Stato o altra Organizzazione) del documento elettronico, che ha il compito di distribuire successivamente i singoli documenti di viaggio agli effettivi titolari, dopo avervi memorizzato i loro dati personali, quali, ad es., dati biografici, foto, ecc.

Il documento può essere visto come costituito da una parte "fisica" (cartacea o plastica, con relativo chip), che consente di verificare visivamente i dati personali del titolare, e da una parte "logica", in cui gli stessi dati sono memorizzati secondo una struttura che ne consenta poi la verifica per mezzo di appositi terminali elettronici con o senza contatto.

L'autenticità e l'integrità del documento e dei relativi dati sono garantiti dall'Ente emettitore. In particolare, la parte fisica del documento, identificata da un numero univoco, è protetta con specifiche misure di sicurezza fisiche, logiche e organizzative, mentre la parte logica è garantita dalla firma digitale dello stesso Ente emettitore.

L'ODV comunica con i terminali elettronici tramite il protocollo Password Authenticated Connection Establishment (PACE), in base a quanto prescritto in [BSI-68].

In generale, i prodotti di questo tipo possono supportare anche il meccanismo di controllo di accesso Basic Access Control (BAC). Tuttavia, un prodotto che implementa l'ODV con il meccanismo BAC agisce al di fuori della politica di sicurezza definita nel TDS.

7.3.1 Architettura dell'ODV

Per una descrizione maggiormente dettagliata dell'ODV, consultare il [TDS]; in particolare:

- le parti, fisica e logica, dell'ODV sono descritte nei par. 1.4.1 e 1.4.3;
- le caratteristiche dell'applicazione sono fornite nel par. 1.4.6;
- il ciclo di vita dell'ODV è costituito da quattro fasi: sviluppo, produzione. personalizzazione e uso operativo, descritte in dettaglio nel par. 1.4.4, incluse le operazioni permesse ad utenti ed amministratori in ciascuna di esse.

7.3.2 Caratteristiche di Sicurezza dell'ODV

7.3.2.1 Compatibilità con la Piattaforma

Alcuni aspetti relativi a funzionalità di sicurezza dell'ODV, inclusi obiettivi di sicurezza, ipotesi, minacce e politiche di sicurezza organizzative definite nel Traguardo di Sicurezza sono coperti direttamente dalla Piattaforma. Per i dettagli consultare il par. 2.5 del [TDS].

7.3.2.2 Funzioni di sicurezza

Le funzioni di sicurezza implementate dall'ODV sono descritte in dettaglio nel par. 7.1 del [TDS]. Di seguito sono riassunti alcuni aspetti ritenuti rilevanti:

- **AccessControl**: l'ODV fornisce un meccanismo di controllo di accesso che consente di definire diverse tipologie di utenti, ciascuna delle quali può svolgere azioni distinte.
- **Authenticate**: ogni azione effettuata per conto di un utente richiede l'identificazione e l'autenticazione preventiva dell'utente stesso; l'ODV garantisce l'uso corretto del meccanismo di autenticazione.
- **SecureManagement_MRTD**: questa funzione gestisce le varie fasi del ciclo di vita dell'ODV, che seguono una sequenza definita e protetta mediante autenticazione.
- **CryptoKey_MRTD**: questa funzione gestisce la generazione di chiavi crittografiche a bordo della piattaforma e la loro sovrascrittura dopo l'uso.

- **AppletParameters_Sign**: alcuni parametri di configurazione e di controllo possono assumere soltanto valori conformi ai requisiti e possono essere firmati, consentendo all'utente di verificarne la sicurezza.

- **Platform**: questa funzione riguarda le funzionalità di sicurezza basate su quelle della libreria crittografica e della piattaforma certificate, non menzionate nelle altre funzioni di sicurezza.

7.4 Documentazione

La documentazione specificata in Appendice A - Indicazioni per l'uso sicuro del prodotto, viene fornita al cliente insieme al prodotto. Per "cliente" del prodotto si intende l'Ente emettitore (Stato o altra Organizzazione) del documento elettronico, che ha il compito di distribuire successivamente i singoli documenti agli effettivi titolari. La documentazione indicata contiene le informazioni richieste per l'installazione, la configurazione e l'utilizzo sicuro dell'ODV in accordo a quanto specificato nel Traguardo di Sicurezza [TDS].

Devono inoltre essere seguite le ulteriori raccomandazioni per l'utilizzo sicuro dell'ODV contenute nel par. 8.2 di questo rapporto.

7.5 Conformità a Profili di Protezione (PP)

L'ODV è un documento di viaggio elettronico costituito da una smart card con o senza contatto programmata in base a requisiti e raccomandazioni definiti dall'International Civil Aviation Organization [ICAO-TR]. Quindi è conforme a due specifici Profili di Protezione (PP):

- BSI-CC-PP-0056-V2-2012 [BSI-56], che definisce gli obiettivi di sicurezza e i requisiti delle smart card con o senzacon o senza contatto utilizzate per documenti di viaggio elettronici (eMRTD), basati sul Rapporto Tecnico "Supplemental Access Control" [ICAO-TR], che utilizzano il meccanismo di controllo di accesso con crittografia Password Authenticated Connection Establishment (PACE), descritto nel documento [ICAO-9303];

- BSI-CC-PP-0068-V2-2011 [BSI-68], che si riferisce alle smart card con o senza contatto con applicativi software utilizzati per realizzare documenti di viaggio, quali ad es. carte dì identità o passaporti elettronici.

7.6 Requisiti funzionali e di garanzia

Tutti i Requisiti di Garanzia (SAR) sono stati selezionati dai CC Parte 3 [CC3].

Il Traguardo di Sicurezza [TDS], a cui si rimanda per la completa descrizione e le note applicative, specifica per l'ODV tutti gli obiettivi di sicurezza, le minacce che questi obiettivi devono contrastare, i Requisiti Funzionali di Sicurezza (SFR) e le funzioni di sicurezza che realizzano gli obiettivi stessi.

Tutti gli SFR sono stati derivati direttamente o ricavati per estensione dai CC Parte 2 [CC2]. In particolare, poiché il TDS dichiara stretta conformità a due PP, sono inclusi anche i componenti estesi definiti in tali PP e precisamente: FIA_API da [BSI-56], FAU_SAS, FCS_RND, FMT_LIM e FPT_EMS da [BSI-68].

7.7 Conduzione della valutazione

La valutazione è stata svolta in conformità ai requisiti dello Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione, come descritto nelle Linee Guida Provvisorie [LGP3] e nelle Note Informative dello Schema [NIS3], ed è stata inoltre condotta secondo i requisiti del Common Criteria Recognition Arrangement [CCRA].

Inoltre, trattandosi di un ODV composito, sono state seguite le indicazioni contenute nel documento "Composite product evaluation for Smart Cards and similar devices" [CCDB], come richiesto dagli accordi internazionali CCRA e SOGIS. Trattandosi di una ri-certificazione, i Valutatori hanno innanzitutto effettuato un'analisi di impatto delle differenze rispetto alla versione già certificata (IDentity Card v3.1/PACE-EAC1), riassumendole nel documento [IAR]. Su questa base, hanno ritenuto ancora validi i risultati della precedente valutazione: in particolare, si precisa che i test di intrusione sono stati completati il 13 gennaio 2015, quindi entro 18 mesi da quelli effettuati per la Piattaforma (luglio 2013, periodo di riferimento indicato nei risultati della relativa certificazione [NSCIB]).

Lo scopo della valutazione è quello di fornire garanzie sull'efficacia dell'ODV nel soddisfare quanto dichiarato nel rispettivo Traguardo di Sicurezza [TDS], di cui si raccomanda la lettura ai potenziali acquirenti. Inizialmente è stato valutato il Traguardo di Sicurezza per garantire che costituisse una solida base per una valutazione nel rispetto dei requisiti espressi dallo standard CC. Quindi è stato valutato l'ODV sulla base delle dichiarazioni formulate nel Traguardo di Sicurezza stesso. Entrambe le fasi della valutazione sono state condotte in conformità ai CC Parte 3 [CC3] e alla CEM [CEM].

L'Organismo di Certificazione ha supervisionato lo svolgimento della valutazione eseguita dall'LVS Systrans.

L'attività di valutazione è terminata in data 8 marzo 2016 con l'emissione, da parte dell'LVS, del Rapporto Finale di Valutazione [RFV], che è stato approvato dall'Organismo di Certificazione il 15 marzo 2016. Successivamente, l'Organismo di Certificazione ha emesso il presente Rapporto di Certificazione.

7.8 Considerazioni generali sulla validità della certificazione

La valutazione ha riguardato le funzionalità di sicurezza dichiarate nel Traguardo di Sicurezza [TDS], con riferimento all'ambiente operativo ivi specificato. La valutazione è stata eseguita sull'ODV configurato come descritto in Appendice B. I potenziali acquirenti sono invitati a verificare che questa corrisponda ai propri requisiti e a prestare attenzione alle raccomandazioni contenute in questo Rapporto di Certificazione.

La certificazione non è una garanzia di assenza di vulnerabilità; rimane una probabilità (tanto minore quanto maggiore è il livello di garanzia) che possano essere scoperte vulnerabilità sfruttabili dopo l'emissione del certificato. Questo Rapporto di Certificazione riflette le conclusioni dell'Organismo di Certificazione al momento della sua emissione. Gli acquirenti (potenziali e effettivi) sono invitati a verificare regolarmente l'eventuale insorgenza di nuove vulnerabilità successivamente all'emissione di questo Rapporto di Certificazione e, nel caso le vulnerabilità possano essere sfruttate nell'ambiente operativo dell'ODV, verificare presso il produttore se siano stati messi a punto aggiornamenti di sicurezza e se tali aggiornamenti siano stati valutati e certificati.

8 Esito della valutazione

8.1 Risultato della valutazione

A seguito dell'analisi del Rapporto Finale di Valutazione [RFV] prodotto dall'LVS e dei documenti richiesti per la certificazione, e in considerazione delle attività di valutazione svolte, come testimoniato dal gruppo di Certificazione, l'OCSI è giunto alla conclusione che l'ODV "IDentity Card v3.2/PACE-EAC1" soddisfa i requisiti della parte 3 dei Common Criteria [CC3] previsti per il livello di garanzia EAL4, con aggiunta di ALC_DVS.2, ATE_DPT.2, AVA_VAN.5, in relazione alle funzionalità di sicurezza riportate nel Traguardo di Sicurezza [TDS] e nella configurazione valutata, riportata in Appendice B.

La Tabella 1 riassume i verdetti finali di ciascuna attività svolta dall'LVS in corrispondenza ai requisiti di garanzia previsti in [CC3], relativamente al livello di garanzia EAL4, con aggiunta di ALC_DVS.2, ATE_DPT.2, AVA_VAN.5.

Classi e componenti di garanzia		**Verdetto**
Security Target evaluation	**Classe ASE**	Positivo
Conformance claims	ASE_CCL.1	Positivo
Extended components definition	ASE_ECD.1	Positivo
ST introduction	ASE_INT.1	Positivo
Security objectives	ASE_OBJ.2	Positivo
Derived security requirements	ASE_REQ.2	Positivo
Security problem definition	ASE_SPD.1	Positivo
TOE summary specification	ASE_TSS.1	Positivo
Development	**Classe ADV**	Positivo
Security architecture description	ADV_ARC.1	Positivo
Complete functional specification	ADV_FSP.4	Positivo
Implementation representation of the TSF	ADV_IMP.1	Positivo
Basic modular design	ADV_TDS.3	Positivo
Guidance documents	**Classe AGD**	Positivo
Operational user guidance	AGD_OPE.1	Positivo
Preparative procedures	AGD_PRE.1	Positivo
Life cycle support	**Classe ALC**	Positivo
Production support, acceptance procedures and automation	ALC_CMC.4	Positivo
Problem tracking CM coverage	ALC_CMS.4	Positivo

Classi e componenti di garanzia		Verdetto
Delivery procedures	ALC_DEL.1	Positivo
Sufficiency of security measures	ALC_DVS.2	Positivo
Developer defined life-cycle model	ALC_LCD.1	Positivo
Well-defined development tools	ALC_TAT.1	Positivo
Test	**Classe ATE**	Positivo
Analysis of coverage	ATE_COV.2	Positivo
Testing: security enforcing modules	ATE_DPT.2	Positivo
Functional testing	ATE_FUN.1	Positivo
Independent testing - sample	ATE_IND.2	Positivo
Vulnerability assessment	**Classe AVA**	Positivo
Advanced methodical vulnerability analysis	AVA_VAN.5	Positivo

Tabella 1 – Verdetti finali per i requisiti di garanzia

8.2 Raccomandazioni

Le conclusioni dell'Organismo di Certificazione sono riassunte nel capitolo 6 - Dichiarazione di certificazione.

Si raccomanda ai potenziali acquirenti del prodotto "IDentity Card v3.2/PACE-EAC1" di comprendere correttamente lo scopo specifico della certificazione leggendo questo Rapporto in riferimento al Traguardo di Sicurezza [TDS].

L'ODV deve essere utilizzato in accordo all'ambiente di sicurezza specificato nel par. 1.4.6.4 del Traguardo di Sicurezza [TDS]. Si assume che, nell'ambiente operativo in cui è posto in esercizio l'ODV, vengano rispettate le Politiche di sicurezza organizzative e le ipotesi descritte nel TDS, in particolare quelle compatibili con la Piattaforma HW dell'ODV (cfr. [TDS], par. 2.5).

Il presente Rapporto di Certificazione è valido esclusivamente per l'ODV nella configurazione valutata; in particolare, l'Appendice A include una serie di raccomandazioni relative alla consegna, all'inizializzazione e all'utilizzo sicuro del prodotto, secondo le indicazioni contenute nella documentazione operativa fornita insieme all'ODV ([CONF, ADM, USR]).

9 Appendice A – Indicazioni per l'uso sicuro del prodotto

La presente appendice riporta considerazioni particolarmente rilevanti per il potenziale acquirente del prodotto.

9.1 Consegna

Poiché l'ODV è di tipo composito, le procedure di consegna prevedono delle interazioni tra lo sviluppatore dell'applicazione (ID&Trust) e il fornitore della Piattaforma (NXP).

In particolare, il fornitore della Piattaforma implementa l'applicazione nel circuito integrato e attiva il processo di inizializzazione e personalizzazione, con la collaborazione dello sviluppatore dell'applicazione. Il documento così creato, cifrato con un'apposita chiave di trasporto, viene inviato al cliente, cioè l'Ente emettitore (Stato o altra Organizzazione) del documento elettronico, tramite un corriere espresso, DHL, TNT, FEDEX, SKY, ecc. Se il documento dovesse perdersi, non potrebbe comunque essere alterato, poiché, dopo che l'applicazione è stata caricata e configurata, è diventato di sola lettura. Infine, l'Ente emettitore consegna successivamente i singoli documenti agli effettivi titolari direttamente presso la propria sede o inviandoli via posta, in base alle normative locali.

La responsabilità di garantire gli aspetti di sicurezza, integrità, confidenzialità e disponibilità, è a carico dello sviluppatore dell'applicazione ID&Trust.

Maggiori dettagli sulla procedura di personalizzazione sono contenuti in:

- IDentity Applet Initialization and configuration Version 3.2.07 [CONF];
- IDentity Applet Administrator's Guide Version 3.2.18 [ADM].

9.2 Installazione e utilizzo sicuro dell'ODV

L'installazione sicura dell'ODV e la preparazione sicura del suo ambiente operativo in accordo agli obiettivi di sicurezza indicati nel [TDS], devono avvenire seguendo le istruzioni contenute nelle apposite sezioni dei seguenti documenti:

- IDentity Applet Initialization and configuration Version 3.2.07 [CONF];
- IDentity Applet Administrator's Guide Version 3.2.18 [ADM];
- IDentity Applet User's Guide Version 3.2.19 [USR].

10 Appendice B – Configurazione valutata

L'ODV è il prodotto “ID&Trust ID Card 3.2: NXP JCOP 2.4.2 R3 Smart Card with ID&Trust IDentity Applet Suite 3.2/PACE-EAC1”, nome abbreviato “IDentity Card v3.2/PACE-EAC1”, sviluppato dalla società ID&Trust.

L’ODV è un prodotto composito e comprende i seguenti componenti HW/SW, con le rispettive versioni, costituenti la configurazione valutata dell’ODV, come riportato in [TDS], a cui si applicano i risultati della valutazione:

- la Piattaforma “NXP J3E120_M65 / J2E120_M65 / J3E082_M65 / J2E082_M65 Secure Smart Card Controller Revision 3”, nome abbreviato “JCOP 2.4.2 R3”, già certificata CC a livello EAL5 con aggiunta di ASE_TSS.2, ALC_DVS.2 e AVA_VAN.5 [NSCIB], a sua volta costituita da:
  - la smart card e lo smart card controller “NXP Secure Smart Card Controllers P5CD145V0v/ V0B(s) and P5CC145V0v/V0B(s)”;
  - la Crypto Library “V2.7/V2.9 on SmartMX P5CD016/021/041/051 and P5Cx081 V1A/V1A(s)”;
  - l’Embedded Software (Java Card Virtual Machine, Runtime Environment, Java Card API, Card Manager);
  - l’applicazione nativa MIFARE (sempre presente fisicamente ma disponibile solo in base alla configurazione)
- la parte applicativa dell’ODV “ID&Trust IDentity Applet Suite Version 3.2”, configurata come applicazione eMRTD;
- la documentazione operativa associata:
  - IDentity Applet Initialization and configuration Version 3.2.07 [CONF]
  - IDentity Applet Administrator’s Guide Version 3.2.18 [ADM]
  - IDentity Applet User’s Guide Version 3.2.19 [USR]

11 Appendice C – Attività di Test

Questa appendice descrive l'impegno dei Valutatori e del Fornitore nelle attività di test. Per il livello di garanzia EAL4, con aggiunta di ALC_DVS.2, ATE_DPT.2, AVA_VAN.5, tali attività prevedono tre passi successivi:

- valutazione in termini di copertura e livello di approfondimento dei test eseguiti dal Fornitore;
- esecuzione di test funzionali indipendenti da parte dei Valutatori;
- esecuzione di test di intrusione da parte dei Valutatori.

Trattandosi di una ri-certificazione, i Valutatori hanno innanzitutto effettuato un'analisi di impatto delle differenze rispetto alla versione già certificata (IDentity Card v3.1/PACE-EAC1), riassumendole nel documento [IAR]. Su questa base, hanno stabilito di dover ri-eseguire le attività relative alle sole famiglie ATE_FUN.1 e ATE_IND.2, mentre hanno ritenuto ancora validi i risultati della precedente valutazione per le famiglie ATE_COV.2 e ATE_DPT.2, che si riportano qui per completezza.

11.1 Configurazione per i Test

Per l'esecuzione dei test è stato predisposto un apposito ambiente di test presso la sede dell'LVS con il supporto del Committente/Fornitore, che ha fornito le risorse necessarie. In particolare, sono stati predisposti una smart card, un lettore di smart card e un PC, sul quale è stato installato lo strumento di test open source "Global Tester, configurato in ambiente di sviluppo Eclipse.

Prima dell'esecuzione dei test il software è stato installato e configurato seguendo le istruzioni contenute nei documenti [CONF], [ADM] e [USR], come indicato nel par. 9.2. Inoltre, trattandosi di un ODV composito, sono state seguite le indicazioni contenute nel documento [CCDB]. In particolare, la Piattaforma hardware è stata già certificata e i relativi risultati sono stati riutilizzati dall'LVS, che ha potuto così valutare direttamente l'applicazione software.

11.2 Test funzionali svolti dal Fornitore

11.2.1 Copertura dei test

Il piano di test presentato dal Fornitore si è basato in gran parte sui seguenti documenti di riferimento, solitamente utilizzati per prodotti tipo passaporti elettronici e simili:

- ICAO RF protocol and application test standard for e-passport - part 3 v.2.01 [ICAO-RF];
- AFNOR BSI contribution to TF4 Amendment to ICAO-TR Technical Report – RF protocol and application test standard for ePassport Part 3, Tests for Application Protocol and Logical Data Structure, Version 1.01, February 2007 Supplemental Access Control Active Authentication [AFNOR-1];

- AFNOR Advanced Security Mechanisms For Machine Readable Travel Documents – Extended Access Control (EAC) Tests For Security Implementation V.1.12, October 3, 2008 [AFNOR-2].

In aggiunta, il Fornitore ha progettato autonomamente altri test aggiuntivi, al fine di dimostrare la completa copertura dei requisiti funzionali SFR e delle funzioni di sicurezza.

11.2.2 Risultati dei test

I Valutatori hanno eseguito una serie di test, scelti a campione tra quelli descritti nel piano di test presentato dal Fornitore, verificando positivamente il corretto comportamento delle TSFI e la corrispondenza tra risultati attesi e risultati ottenuti per ogni test.

11.3 Test funzionali ed indipendenti svolti dai Valutatori

Successivamente, i Valutatori hanno progettato dei test indipendenti per la verifica della correttezza delle TSFI.

Non sono stati utilizzati strumenti di test particolari oltre ai componenti dell'ODV che hanno permesso di sollecitare tutte le TSFI selezionate per i test indipendenti.

Nella progettazione dei test indipendenti, i Valutatori hanno considerato aspetti che nei test del Fornitore erano non presenti o ambigui o inseriti in test più complessi che interessavano più interfacce contemporaneamente ma con un livello di dettaglio non ritenuto adeguato.

I Valutatori, infine, hanno anche progettato ed eseguito alcuni test in modo indipendente da analoghi test del Fornitore, sulla base della sola documentazione di valutazione.

Infine, trattandosi di un ODV composito, sono stati eseguiti anche i test integrativi miranti a verificare il comportamento dell'ODV nel suo complesso, svolgendo le attività integrative previste dalla famiglia ATE_COMP, in base a quanto indicato nel documento [CCDB].

Tutti i test indipendenti eseguiti dai Valutatori hanno dato esito positivo.

11.4 Analisi delle vulnerabilità e test di intrusione

Trattandosi di una ri-certificazione, i Valutatori, sulla base dell'analisi di impatto [IAR] delle differenze rispetto alla versione già certificata, hanno ritenuto ancora validi i risultati dei test di intrusione effettuati nella precedente valutazione, che si riportano qui per completezza.

Per l'esecuzione di queste attività è stato utilizzato lo stesso ambiente di test già utilizzato per le attività dei test funzionali (cfr. par. 11.1). I Valutatori hanno innanzitutto verificato che le configurazioni di test fossero congruenti con la versione dell'ODV in valutazione, cioè quella indicata nel [TDS], par. 1.4.

In una prima fase, i Valutatori hanno effettuato delle ricerche utilizzando varie fonti di pubblico dominio, quali internet, libri, pubblicazioni specialistiche, atti di conferenze, comprese le varie edizioni dell'ICCC, documenti JIL e CCDB, ecc., al fine di individuare eventuali vulnerabilità note applicabili a tipologie di prodotti simili all'ODV, cioè documenti elettronici eMRTD. Sono state così individuate diverse vulnerabilità potenziali, la maggior

parte delle quali, però, si riferiscono alla Piattaforma hardware già certificata EAL5+, e quindi non sfruttabili con potenziali di attacco High, come previsto in AVA_VAN.5.

In una seconda fase, i Valutatori hanno esaminato i documenti di valutazione (TDS, specifiche funzionali, progetto dell'ODV, architettura di sicurezza e documentazione operativa, compresa quella della Piattaforma) al fine di evidenziare eventuali ulteriori vulnerabilità potenziali dell'ODV. Da questa analisi, congiuntamente a quella del codice sorgente, i Valutatori hanno effettivamente determinato la presenza di altre vulnerabilità potenziali; anche in questo caso, però, la maggior parte di esse sono state già considerate nel corso della valutazione della Piattaforma, come documentato nel relativo Rapporto Finale [ETR-COMP].

I Valutatori hanno analizzato nel dettaglio le potenziali vulnerabilità individuate nelle due fasi precedenti, per verificare la loro effettiva sfruttabilità nell'ambiente operativo dell'ODV. Quest'analisi ha portato a individuare sei effettive vulnerabilità potenziali.

I Valutatori hanno quindi progettato dei possibili scenari di attacco, con potenziale di attacco High, e dei test di intrusione per verificare la sfruttabilità di tali vulnerabilità potenziali candidate. I test di intrusione sono stati descritti con un dettaglio sufficiente per la loro ripetibilità avvalendosi a tal fine delle schede di test, utilizzate in seguito, opportunamente compilate con i risultati, anche come rapporto dei test stessi.

Trattandosi di un ODV composito, sono state eseguite anche le attività integrative previste dalla famiglia AVA_COMP, in base a quanto indicato nel documento [CCDB], al fine di verificare il comportamento dell'ODV nel suo complesso.

Dall'esecuzione dei test di intrusione, i Valutatori hanno effettivamente riscontrato che nessuno scenario di attacco con potenziale High può essere portato a termine con successo nell'ambiente operativo dell'ODV nel suo complesso. Pertanto, nessuna delle vulnerabilità potenziali precedentemente individuate può essere effettivamente sfruttata. Non sono state individuate neanche vulnerabilità residue, cioè vulnerabilità che, pur non essendo sfruttabili nell'ambiente operativo dell'ODV, potrebbero però essere sfruttate solo da attaccanti con potenziale di attacco superiore a High.