



2N PICard Commander

Manuale d'uso



Indice

Simboli e termini utilizzati	3
Descrizione del prodotto	4
prodotti correlati	5
Dispositivi compatibili	6
Installazione e caricamento della licenza	8
Collegamento di un altro lettore	8
Progetto	9
Creazione di un nuovo progetto	9
Apertura del progetto	9
Impostazioni del progetto	9
Impostazioni di base (Basic settings)	9
Chiave di crittografia principale (Main Encryption Key)	9
Modalità di crittografia (Card mode)	10
Salva su disco	11
Crittografia e lettura delle carte	12
Crittografia della carta	12
Esportazione delle chiavi di lettura	13
Esporta le chiavi su file	13
Carica le chiavi su Access Commander	14
Lettura delle informazioni sulla carta	14
Cancellazione dei dati sulla scheda	15
Licenze di terze parti	16

Simboli e termini utilizzati

Nel manuale vengono utilizzati i seguenti simboli e pittogrammi:



PERICOLO

Rispetta sempre queste istruzioni per evitare il rischio di lesioni.



AVVERTIMENTO

Rispetta sempre queste istruzioni per evitare danni al dispositivo.



ATTENZIONE

Avvertimento importante. La mancata osservanza delle istruzioni potrebbe causare il malfunzionamento del dispositivo.



SUGGERIMENTO

Informazioni utili per un utilizzo o una configurazione più semplice e veloce.



NOTA

Procedure e consigli per un utilizzo efficace delle funzionalità del dispositivo.

Descrizione del prodotto

2N PICard Commander è un'applicazione software per crittografare le credenziali sulle carte di accesso. L'applicazione crea progetti che generano un set di chiavi di crittografia e lettura. Le chiavi del lettore di progetto possono essere importate nei dispositivi 2N o in Access Commander, che successivamente garantisce la distribuzione delle chiavi di lettura ai dispositivi 2N collegati.

Tecnologia 2N PICard è destinato alla crittografia della carta MIFARE® DESFire® EV2 E MIFARE® DESFire® EV3.

Nell'app PICard Commander è possibile cancellare i dati registrati sulle tessere di accesso.

Funzionalità dell'applicazione PICard Commander è subordinato all'acquisto di una licenza.

prodotti correlati

Numero d'ordine: 91379601

Licenza 2N PICard Commander

La licenza viene sempre rilasciata per un determinato lettore di carte USB in base alla chiave del dispositivo del lettore indicato. I lettori di chiavi del dispositivo possono essere trovati prima di caricare la licenza PICard Commander. I lettori di schede USB supportati sono elencati di seguito.



Numero d'ordine: 9137421E

Lettore USB di tessere RFID 13,56 MHz, 125 kHz e dispositivi NFC/HCE

Lettore di carte RFID esterno per collegamento a PC tramite interfaccia USB. Adatto per la gestione del sistema e l'aggiunta di schede da 13,56 MHz, 125 kHz e dispositivi Android con supporto NFC/HCE tramite interfaccia web o app del citofono IP 2N Accedi al comandante. Adatto per caricare le carte MIFARE DESFire su un'applicazione di crittografia PICard Commander^a. Legge gli stessi tipi di carte e dispositivi dei lettori di carte dei citofoni IP 2N:

Schede RFID supportate 125 kHz:

- EM4x02
- NXP HiTag2

Schede RFID supportate 13,56 MHz:

- **ISO14443A** (MIFARE Classic, MIFARE Plus, MIFARE Mini, MIFARE Ultralight, MIFARE DESFire CSN only)
- **PicoPass** (HID iClass CSN, Picopass)
- **FeliCa** (Standard, Lite)
- **ST SR** (SR, SRI, SRIX)
- **Mobile Key**



Numero d'ordine: 9137424E

Protetto Lettore USB di tessere RFID 13,56 MHz, 125 kHz e dispositivi NFC/HCE

Lettore esterno di carte RFID sicuro per il collegamento al PC tramite interfaccia USB. Adatto per la gestione del sistema e l'aggiunta di schede da 13,56 MHz, 125 kHz e dispositivi Android con supporto NFC/HCE tramite interfaccia web o app del citofono IP 2N Access Commander. Adatto per caricare le carte MIFARE DESFire su un'applicazione di crittografia 2N PICard Commanderanno^a. Legge gli stessi tipi di carte e dispositivi dei lettori di carte dei citofoni IP 2N:

125 kHz

- EM4xxx
- HID Prox

13,56 MHz

- ISO14443A (MIFARE DESFire)
- PicoPass (HID iClass)
- FeliCa

Descrizione del prodotto

- ST SR(IX)
- 2N Mobile Key
- HID SE (Seos, iClass SE, MIFARE SE)



Numero d'ordine: 11202601

Scheda RFID 2N MIFARE Desfire EV3 4K 13,56MH 10 pz.

confezione da 10 pz

MIFARE DESFire EV3 (ISO14443A)

Numero d'ordine: 11202602

Portachiavi RFID 2N MIFARE Desfire EV3 4K 13,56 MHz 10 pz.

confezione da 10 pz

MIFARE DESFire EV3 (ISO14443A)



^aTecnologia 2N PICard è destinato alla crittografia delle carte MIFARE DESFireEV2 e MIFARE DESFire EV3.

Dispositivi compatibili

Le carte con tecnologia PICard possono essere lette sui seguenti dispositivi:

2N IP Style

- 2N IP Style main unit
(codice ordine 9157101)
- 2N IP Style main unit, secured
(codice ordine 9157101-S)

2N IP Verso

- 2N IP Verso – 13.56MHz secured card reader, NFC, reads UID + PACS ID
(codice ordine 9155086/9155042)
- 2N IP Verso Bluetooth & RFID reader 125kHz, 13.56MHz, NFC
(codice ordine 91550945)
- 2N IP Verso Bluetooth & RFID reader 125kHz, secured 13.56MHz, NFC
(codice ordine 91550945-S)
- 2N IP Verso Touch keypad & RFID reader 125kHz, 13.56MHz, NFC
(codice ordine 91550946)
- 2N IP Verso Touch keypad & RFID reader 125kHz, secured 13.56MHz, NFC
(codice ordine 91550946-S)

2N Access Unit

- 2N Access Unit 2.0 13.56 MHz, NFC
(codice ordine 9160342)
- 2N Access Unit 2.0 secured 13.56 MHz, NFC
(codice ordine 9160342-S)
- 2N Access Unit 2.0 125kHz, 13.56MHz, NFC
(codice ordine 9160344)
- 2N Access Unit 2.0 125kHz, secured 13.56MHz, NFC
(ordine n. 9160344-S)
- 2N Access Unit 2.0 Bluetooth & RFID – 125kHz, 13.56MHz, NFC
(codice ordine 9160345)
- 2N Access Unit 2.0 Bluetooth & RFID – 125kHz, secured 13.56MHz, NFC
(codice ordine 9160345-S)

Descrizione del prodotto

- 2N Access Unit 2.0 Touch keypad & RFID – 125kHz, 13.56MHz, NFC
(codice ordine 9160346)
- 2N Access Unit 2.0 Touch keypad & RFID – 125kHz, secured 13.56MHz, NFC
(codice ordine 9160346-S)

2N Access unit M

- 2N Access Unit M 13.56 MHz, NFC ready
(codice ordine 916112)
- 2N Access Unit M RFID – 125kHz, 13.56MHz, NFC
(ordine n. 916114)
- 2N Access Unit M Bluetooth & RFID – 125kHz, 13.56MHz, NFC
(codice ordine 916115)
- 2N Access Unit M Touch keypad & RFID – 125kHz, 13.56MHz, NFC
(codice ordine 916116)

2N IP Force

- 2N IP Force 13.56MHz card reader, NFC ready, reads UID
(codice ordine 9151031)
- 2N IP Force 13.56MHz card reader, NFC ready, reads UID + PACS ID
(codice ordine 9151031S)

Installazione e caricamento della licenza

1. Installalo PCard Commander nel solito modo tramite il programma di installazione.
2. Dopo aver avviato l'applicazione, caricare la licenza facendo clic su **Load License** nella barra arancione (o nella scheda Help > License). Quindi caricare il file di licenza dal disco. Per caricare correttamente la licenza, il lettore di carte deve essere collegato al computer.



NOTA

La licenza è legata ad uno specifico lettore di schede USB. Per ottenere una licenza è quindi necessario inserire la Device Key del dispositivo lettore, reperibile nelle informazioni sulla licenza in PCard Commander (Help > License). Il lettore di carte deve essere collegato al computer per visualizzare la chiave.



Device key of connected reader:

324e-4142-003c0061000d513634353830

Collegamento di un altro lettore

Se al computer viene collegato un lettore diverso da quello abbinato alla licenza in uso, l'app PCard Commander ti avviserà dopo l'avvio. Puoi caricare una nuova licenza nella scheda Help > License.

Progetto

La creazione di singoli progetti consente di crittografare gruppi di carte di accesso in diverse modalità. Puoi impostare ciascun progetto specificatamente allo scopo di utilizzare le carte. Il progetto genera una serie di chiavi di crittografia e lettura. Al dispositivo o a Access Commander puoi caricare le chiavi di lettura di un solo progetto alla volta.

Creazione di un nuovo progetto

Dopo aver aperto l'applicazione, premere il pulsante per creare un nuovo progetto **Start new project**.

Modo alternativo: segnalibro *File > New project*

Si aprirà una procedura guidata per la configurazione di un nuovo progetto, seguire i passaggi seguenti [Impostazioni del progetto \[9\]](#).

Apertura del progetto

1. Nell'interfaccia iniziale dell'applicazione, fare clic sul pulsante **Open project**.

Modo alternativo: segnalibro *File > Open project*

I progetti aperti più di recente vengono visualizzati nella sezione inferiore dell'interfaccia iniziale dell'applicazione.

Impostazioni del progetto

Quando si avvia un progetto è necessario impostarne i parametri.

Le impostazioni possono essere modificate successivamente nella Configurazione progetto nell'interfaccia iniziale dell'applicazione (percorso alternativo: scheda Project > Change configuration).

Impostazioni di base (Basic settings)

- **Project name** – nome del progetto
- **Project description** – spazio per inserire note sul progetto

Chiave di crittografia principale (Main Encryption Key)

Secondo la chiave di crittografia principale (MEK) viene generata dall'applicazione PICard Commander un set di chiavi per crittografare i dati di accesso della carta. La chiave dovrebbe quindi essere unica e sufficientemente sicura. Il set di chiavi è basato sulla chiave di crittografia master, quindi i progetti con la stessa chiave di crittografia master generano gli stessi set di chiavi. Se si perde un progetto è possibile crearne uno nuovo con la stessa chiave di crittografia master e proseguire con la crittografia delle altre carte. Le chiavi di lettura del progetto smarrito già caricate sul dispositivo 2N saranno valide anche per le carte appena crittografate.



AVVERTIMENTO

La chiave di crittografia principale non può essere successivamente **visualizzare o modificare**.



SUGGERIMENTO

Per la massima sicurezza, è importante salvare sia il file di progetto stesso che la chiave di crittografia principale (MEK). L'ideale è conservare la chiave di crittografia principale (MEK) in modo sicuro lontano dall'ambiente online, ad esempio in una cassaforte, in una cassetta di sicurezza, ecc.

Modalità di crittografia (Card mode)

È possibile scegliere tra le seguenti modalità di crittografia della carta:

- **Card may be used for other applications later on (best compatibility)** – Le carte verranno utilizzate principalmente dai sistemi 2N. I dati sulla carta verranno crittografati, ma il suo UID rimarrà leggibile da applicazioni di terze parti. Le carte possono essere riformattate al loro stato originale.
- **Card will be used only for access control with 2N devices (best privacy)** – Le carte verranno utilizzate esclusivamente nei sistemi 2N. I parametri della scheda verranno ripristinati in modo permanente. Una volta crittografata, sulla carta viene attivata la funzione ID casuale.
- **Card is already used for other applications (advance settings)** – Sulle carte sono già caricate applicazioni di terzi. Nel passaggio successivo è possibile impostare i parametri selezionati delle carte MIFARE DESFire di cui dispone la tecnologia 2N PICard da crittografare nel progetto.



NOTA

Selezione della modalità **Card is already used for other applications** è irreversibile.

Nel passaggio successivo è possibile compilare:

- Application ID (AID) – il codice sotto il quale sarà presentata la domanda 2N PICard identificato sulla carta. L'AID è preimpostato su 53324E.
- **PICC master key type** – il tipo di chiave master PICC impostata sulle carte di cui dispone l'applicazione 2N Picard crittografare.
- **PICC master key** – il valore delle tessere master PICC di cui dispone l'applicazione 2N Picard crittografare.
- **Enable randomisation of readable card ID** - l'attivazione della funzione ID casuale garantisce che l'UID della carta cambi in modo casuale ogni volta che viene caricata. Pertanto, una persona non autorizzata non può utilizzare impropriamente la carta per identificarne il titolare.
- **Encrypt cards in factory default state (change default PICC master key)** – opzione per caricare la chiave master PICC specificata su altre carte vuote durante la crittografia nel progetto. Se questa opzione non è selezionata, PICard Commander rifiuterà di crittografare una carta vuota.



AVVERTIMENTO

- Dopo il processo di crittografia delle carte con il nuovo AID, le chiavi del lettore devono essere nuovamente esportate. Le carte precedentemente crittografate con il vecchio AID diventeranno illeggibili dai dispositivi 2N.
- La modifica della chiave master PICC in un progetto con carte già crittografate renderà impossibile modificare ulteriormente queste carte nel progetto e cancellare i loro dati. La validità delle carte per l'autenticazione nei dispositivi 2N non sarà influenzata dalla modifica.
- L'attivazione della funzione Carta d'identità casuale è irreversibile. L'UID originale della carta rimane illeggibile anche dopo la formattazione della carta.

Salva su disco

Il file di progetto viene salvato su disco come *Nome del progetto.picprj*.

Selezionando la casella **Protect project file with password** consente di impostare una password per aprire il progetto. La password può essere modificata successivamente nella scheda Project > Change protection password.



AVVERTIMENTO

Non potrai dimenticare la password in seguito **visualizzare o ripristinare**.

Crittografia e lettura delle carte

Ecco una panoramica di ciò che troverai nel capitolo:

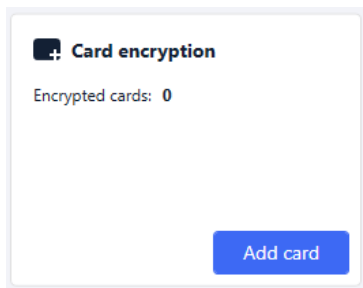
- [Crittografia della carta \[12\]](#)
- [Esportazione delle chiavi di lettura \[13\]](#)
- [Lettura delle informazioni sulla carta \[14\]](#)
- [Cancellazione dei dati sulla scheda \[15\]](#)

Crittografia della carta

Il processo di crittografia delle carte in PICard Commander assegna a ciascuna carta un identificatore univoco a 128 bit, che viene poi crittografato utilizzando le chiavi di crittografia del rispettivo progetto. Nel progetto è possibile caricare la carta e così scoprire l'identificatore assegnato, eventualmente altre informazioni sulla carta e se è possibile crittografarla nel progetto.

Processo di crittografia

1. Nell'interfaccia iniziale dell'applicazione, fare clic su **Add card** nella sezione **Card encryption**.
Modo alternativo: segnalibro *Project > Encrypt New Card*



Credential ID for new card – nuovo identificativo della carta caricata

2. Posiziona la carta sul lettore. Premendo il pulsante **Encrypt** alla carta vengono assegnati i dati di accesso, che vengono contemporaneamente crittografati.



SUGGERIMENTO

Spuntando la casella a destra, puoi avviare la crittografia automatica delle altre carte allegate senza dover premere nuovamente il pulsante **Encrypt**.

L'applicazione informa sull'avvenuta crittografia della carta.

Se non è stato possibile crittografare la carta, l'applicazione ne informa il motivo:

- **Card cannot be encrypted** – applicazione PICard Commander non ha accesso alla tessera master PICC. Se desideri crittografare le carte con una chiave master PICC preimpostata, devi selezionare la modalità di crittografia appropriata in [Impostazioni del progetto \[9\]](#).
- **Not enough free space on card** – non c'è abbastanza spazio sulla carta per caricare la tecnologia 2N PICard. La memoria minima richiesta è 512 B.
- **Unsupported card** – l'applicazione non supporta questo tipo di carta. Tecnologia 2N PICard è progettato per crittografare le carte MIFARE DESFire EV2 ed EV3.
- **Only MIFARE DESFire EV2 or EV3 are supported** – l'applicazione non supporta questo tipo di carta. La scheda caricata è MIFARE DESFire EV1.
- **Communication failure with card** – il lettore non è riuscito a leggere la tessera. Posiziona la carta contro il lettore e non rimuoverla fino al completamento del processo di crittografia.



SUGGERIMENTO

Nella sezione inferiore della finestra è presente un elenco a discesa degli identificatori della carta crittografati. Se vuoi salvare l'elenco, copialo prima di chiudere la finestra. Chiudendo la finestra si cancella l'elenco. Successivamente gli identificatori potranno essere visualizzati solo per le singole carte.

Esportazione delle chiavi di lettura

Affinché i dispositivi 2N possano accedere ai dati sulle carte crittografate, devono conoscere le chiavi di lettura del progetto. Dall'app PICard Commander può leggere le chiavi essere esportate sul dispositivo 2N o su Access Commander, che fornisce la distribuzione a tutti i dispositivi 2N collegati. Una volta caricate le chiavi del lettore sul dispositivo, i dispositivi saranno in grado di leggere le carte crittografate nel progetto specifico dopo il caricamento delle chiavi del lettore.

1. Nell'interfaccia iniziale dell'applicazione, fare clic su **Export** nella sezione Reader keys export (percorso alternativo: tab Project > Export reader keys).
2. Puoi esportare le chiavi del lettore di progetto in due modi:
 - [Esporta le chiavi su file \[13\]](#)
 - [Carica le chiavi su Access Commander \[14\]](#)



ATTENZIONE

Se si collega nuovamente il modulo di espansione del lettore di carte RFID al dispositivo 2N, in cui sono caricate le chiavi di lettura, utilizzando un cavo VBUS, questo modulo deve essere accoppiato con il dispositivo. Puoi associare il modulo di espansione del lettore tramite l'interfaccia web del dispositivo nella sezione Hardware, nel menu Moduli di espansione.

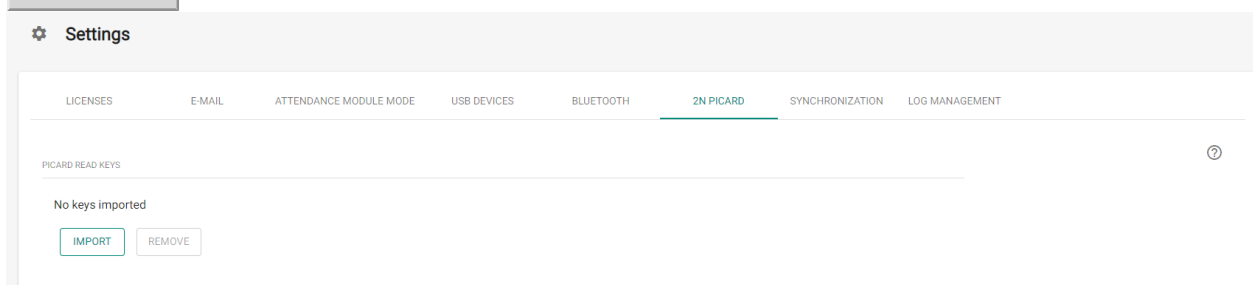



Esporta le chiavi su file

L'applicazione genera un file chiave e lo salva su disco. Il file deve quindi essere importato nelle impostazioni del dispositivo 2N o in Access Commander attraverso le loro interfacce web. Nella fase successiva dell'esportazione è possibile impostare una password per il file salvato.

- **Importa in Access Commander (versione 3.00 e successive)** tramite l'interfaccia web: Impostazioni > Accesso > scheda PICard > **Importare**

- **Importa in Access Commander** tramite interfaccia web: Impostazioni di sistema > 2N PICARD > sezione **IMPORTARE**



- **Importa sul dispositivo 2N** tramite l'interfaccia web: sezione Servizi > menu Controllo Accessi > scheda PICArd > 

Carica le chiavi su Access Commander

Applicazione PICArd Commander carica le chiavi di lettura direttamente su Access Commander, che garantisce la successiva distribuzione ai dispositivi 2N collegati. Nel passaggio successivo è necessario inserire i dati di accesso dell'amministratore per la licenza Access Commander.

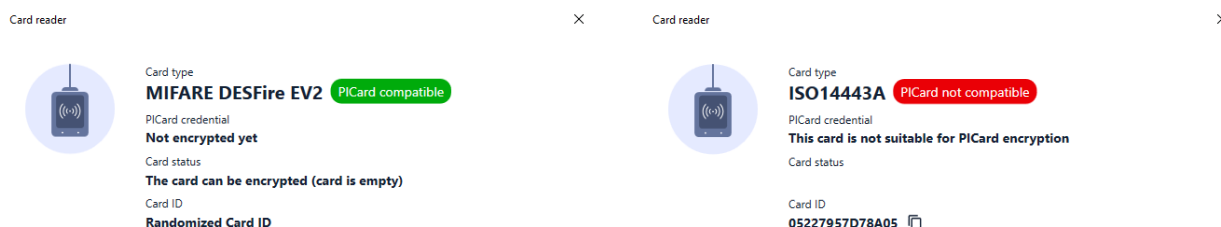
Address – Indirizzo HTTP dell'interfaccia web Access Commander

Login name – nome di accesso dell'account amministratore Access Commander

Password – password di accesso per l'account specificato Access Commander

Lettura delle informazioni sulla carta

Nella scheda è possibile visualizzare l'identificatore della carta assegnato e altre informazioni sulla carta e le sue opzioni di crittografia *Project > Read Card*. Le informazioni vengono lette quando la carta viene applicata al lettore.



Questa carta può essere crittografata nell'applicazione.

Questo tipo di carta non può essere crittografata nell'applicazione.

PICard credential recupera l'identificatore della carta assegnato durante il processo di crittografia. Se la carta non ha un identificatore, verranno visualizzate le informazioni sulle sue opzioni di assegnazione:

- **Not encryptable** – il tipo di carta è compatibile con la tecnologia 2N PICard, ma il progetto non ha accesso alla sua chiave principale PICC.
- **This card is not suitable for PICard encryption** – l'applicazione non supporta questo tipo di carta. Tecnologia 2N PICard è destinato alla crittografia delle carte MIFARE DESFire EV2 ed EV3.
- **Not encrypted yet** – la carta può essere crittografata.
- **Unknown** – la carta è crittografata in un altro progetto con una chiave di crittografia principale diversa. La carta potrebbe anche essere danneggiata.

Card Status mostra lo stato o le opzioni di crittografia della carta specificata:

- **Valid PICard credential** – la carta è crittografata in questo progetto.

- **The card can be encrypted (card is empty)** – la carta non è crittografata. Sulla scheda sono presenti le impostazioni di fabbrica.
- **The card can be encrypted** – la carta non è crittografata. Sulla scheda è impostata una chiave master PICC compatibile con questo progetto.
- **Different PICC Master Key detected. Card's current PICC Master Key required for encryption** – la carta non può essere crittografata in questo progetto. La chiave principale PICC impostata è diversa.
- **PICard application created in a different project, so cannot be read in this project**– la carta è crittografata in un altro progetto.
- **Only MIFARE DESFire EV2 or EV3 are supported** – la carta non può essere crittografata. L'applicazione non supporta questo tipo di carta. La scheda caricata è MIFARE DESFire EV1.
- **INVALID CREDENTIAL (there's a problem with the digital signature)** – i dati di accesso crittografati della carta non possono essere visualizzati. Non è stato possibile confermare la loro autenticità. La firma digitale non è valida.

Card ID visualizza l'UUID della carta o segnala che la funzione ID casuale è attiva.

Cancellazione dei dati sulla scheda

Applicazione PICard Commander consente di formattare le carte o cancellare i loro dati di accesso crittografati. Le carte possono essere cancellate e formattate solo nel progetto in cui sono crittografate.

Formattazione della scheda



AVVERTIMENTO

La formattazione della scheda cancellerà tutti i dati sulla scheda, inclusi i dati di terze parti.

1. Apri la scheda Progetto > Formato scheda. Posizionare la carta contro il lettore. Premendo il pulsante **Format card** la scheda verrà formattata.



NOTA

Se sulla scheda è abilitata la funzione ID casuale, la formattazione della scheda non ripristinerà la leggibilità dell'UID originale.

Cancellazione dei dati di accesso

Erase card

×



Formatting will erase PICard and all other applications on the card. To remove PICard without affecting other applications, please select 'Only delete PICard application'



Card can be formatted.
Click button to continue.

Delete PICard

Only delete PICard application

1. Apri la scheda Project > Format card.
2. Selezionare la casella **Only delete PICard application**.
3. Posizionare la carta contro il lettore.
4. Premendo il pulsante **Delete PICard** i dati di accesso crittografati della carta verranno cancellati.

Licenze di terze parti

Un elenco completo delle licenze di libreria di terze parti utilizzate è disponibile nella scheda Help > About.

2N



wiki.2n.com

2N PICard Commander – Manuale d'uso

© 2N Telekomunikace a. s., 2024

[2N.com](https://2n.com)