TS Cards and Readers for Access Control User Guide

VIP Program for Identiv's TS Cards and Readers

December 6, 2019

This user guide introduces the VIP Program for Identiv's TS Cards and Readers and outlines the process for customers to request custom cryptographic keys for their physical access control deployment.

Introduction

Identiv's TS Cards (and compatible TS Readers) are a turnkey solution for physical access control with the ability to support future applications that complement access control. Identiv's TS solution is comprised of a TS Card (also called "credential") and a compatible TS Reader that provides a protected, encrypted contactless transaction before opening a door.

Identiv's TS products are the newest generation of secure, open products for protecting any access control deployment. TS can be used to migrate from low-frequency (LF) proximity 125 KHz technology to more advanced, high-assurance solutions (i.e., anti-cloning of access badges). Although TS Cards and Readers are designed to work together, Identiv enables third-party card or reader manufacturers to provide TS-compatible cards and readers in the future.

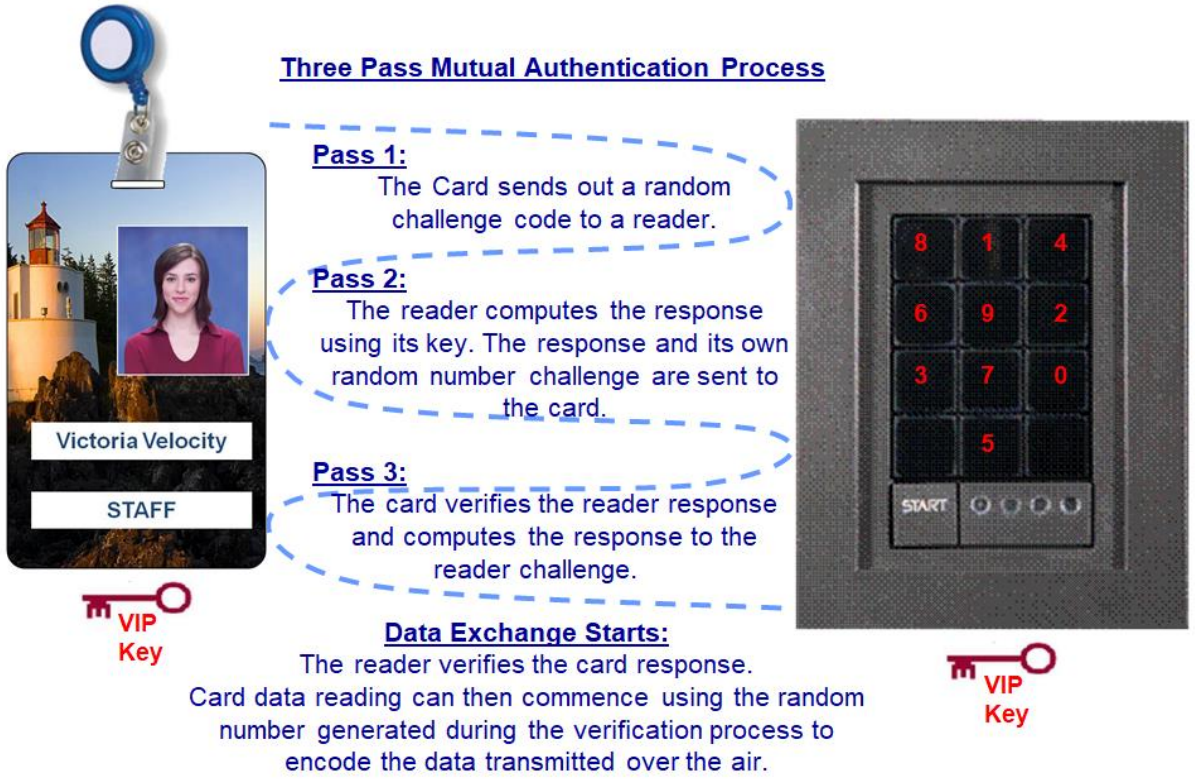
If you are new to the Identiv's TS concept, please refer to identiv.com/products/credentials/ts-cards/ and identiv.com/products/physical-access/readers/ts-reader-family/.

To protect user information, TS leverages state-of-the-art security based on NXP MIFARE DESFire® technology, an open platform that stores all types of data, including data for physical access control. NXP technology is widely used in transportation, closed-loop payment, hospitality, university cards, ticketing, and other markets. The MIFARE DESFire ecosystem of partners makes it the most open smart card platform available today and provides premium security assurance with NIST's approved AES-symmetric chip cryptography.

What Is VIP?
All TS Cards and Readers come with a standard set of AES-128 keys generated and handled by Identiv. Although this model provides immediate compatibility between all TS Cards and Readers, organizations can request a more configurable security model where proprietary application keys can be utilized.

Identiv's VIP Program addresses this challenge by offering an infrastructure for TS Cards and Readers programmed with a customer's keys for maximum control and security in their deployment.

How Does It Work?
DESFire authentication protocol with symmetric keys:



Cryptographic Key Handling

TS Cards and Readers are provisioned at Identiv's U.S. facility in Santa Ana, California. Identiv's manufacturing plant acts as a Cards Service Bureau for central issuance of any TS products. For more information, please refer to identiv.com/products/credentials/utrust-cards-service-bureau/.

Identiv's Cards Service Bureau encompasses a series of products that include card printers, various chip encoders, as well as Identiv's ITS product. ITS is a hosted, cloud-based system designed to securely issue credentials and readers loaded with TRN firmware. A FIPS140-2 L3-approved hardware security module (HSM) is part of the ITS system. The HSM is a high-protected hardware that acts like a smart card with ample space for handling keys of any type. The HSM stores all necessary AES keys for any card deployment, such as Identiv's default TS keys or a customer's VIP key.

It is essential to have reliable, secure mechanisms in place to protect an organization's most precious assets — cryptographic keys.

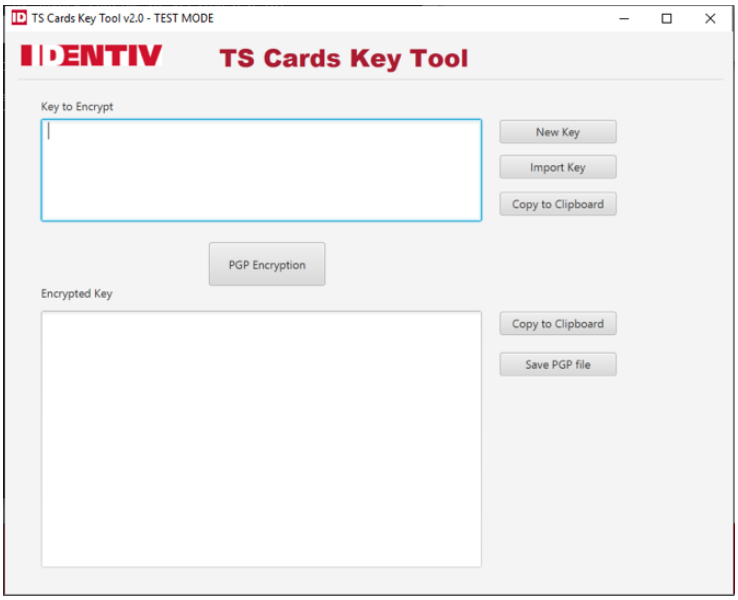
Cryptographic Key Exchange

There are several different ways to share cryptographic keys: simple PGP files via email, password-encrypted zipped files, and the full-blown key ceremony process. As a trade-off between affordability, usability, and security level, Identiv has adopted a public key infrastructure (PKI)-enabled model using PGP encryption. Other models, including a key ceremony, can be supported but at an additional cost. Please reach out to your Identiv Sales Representative to continue a discussion on key ceremonies.

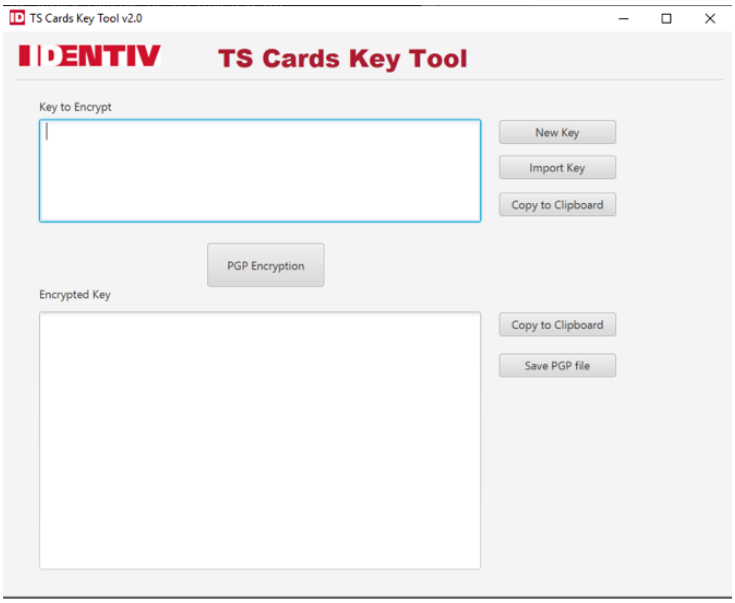
In Identiv's VIP model, we recommend using Identiv's TS Cards Key Tool. The tool is available in two versions, depending on if the customer is transferring a TEST key or PRODUCTION (PROD) key. A TEST key will be injected into the Identiv's TEST HSM during the validation phase, while a PROD key must only be exchanged with the tool to encrypt production keys. Each tool employs different Identiv PGP keys, respectively Identiv TS TEST PGP Key or Identiv TS PROD PGP Key.

The tool is available via FTP or at http://files.identiv.com/products/credentials/ts-cards/TS-VIP-Key-Tool-ProductionKey.7z.

Main Screen for the TS Cards Key Tool (TEST key):



Main Screen for the TS Cards Key Tool (PROD key):



Identiv's TS Cards Key Tool provides all necessary functions to manually create or import AES-128 keys. It is designed to transfer as many keys as needed in the end-user's application. It is recommended that end-users generate their own keys and transfer them encrypted to the Identiv team (described below). However, the Identiv team can generate keys on an end-user's behalf and import them in a similar way to our HSM.

For a TS Card, the end-user must use Identiv's TS Cards Key Tool to create three (3) key files for the HSM:

- PICC key
- App Write key
- App Read key

All tool options are described below:

- New Key: Create AES-128 bit key
- Import Key: Import the key from your own file
- PGP Encryption: Encrypt the key and display the value on the "Encrypted Key" text area
- Save PGP File: Save the key output as a PGP file and share the PGP encrypted file for importing to HSM

All files containing the encrypted keys are attached with the ".pd" extension and will be directly injected by Identiv team into the target HSM.

As part of the process, it is requested to have one .pd file for each AES-128 key transferred to Identiv. There is a minimum of three (3) keys for a TS Card application. If a customer requests to load applications in addition to the standard TS Card application to the cards with specific keys attached to those applications, additional individual keys (and .pd files) will have to be generated.

Naming convention for the ".pd" key files:

XXXXX-VIP-Desfire-YYYY-PICC-ZZZ.pg

- XXXX: Customer alias on up to 5 letters
- YYYY: TEST or PROD
- ZZZ: Version number of the key (start with 001)

Example for TEST key for customer HIRSCH:

- HIRSCH-VIP-Desfire-TEST-PICC-001.pg
- HIRSCH-VIP-Desfire-TEST-AppMK0-001.pg
- HIRSCH-VIP-Desfire-TEST-AppMK1-001.pg

Example for PROD key:

- HIRSCH-VIP-Desfire-PROD-PICC-001.pg
- HIRSCH-VIP-Desfire-PROD-AppMK0-001.pg
- HIRSCH -VIP-Desfire-PROD-AppMK1-001.pg

Once all files are issued, please send to uTrustVipKey@identiv.com and copy sardiley@identiv.com. An Identiv Representative will confirm after the corresponding keys are properly injected in the HSM.

TS Card Part Numbers

All standard TS Card part numbers are formatted this way:

- 5020-AAAAA-001

For VIP-managed TS Cards, the part number will become “5020-AAAAA-VIP-XXXXX-YYYY-ZZZ”:

- XXXXX: Same as above (customer name)
- YYYY: TEST or PROD
- ZZZ: Version Number

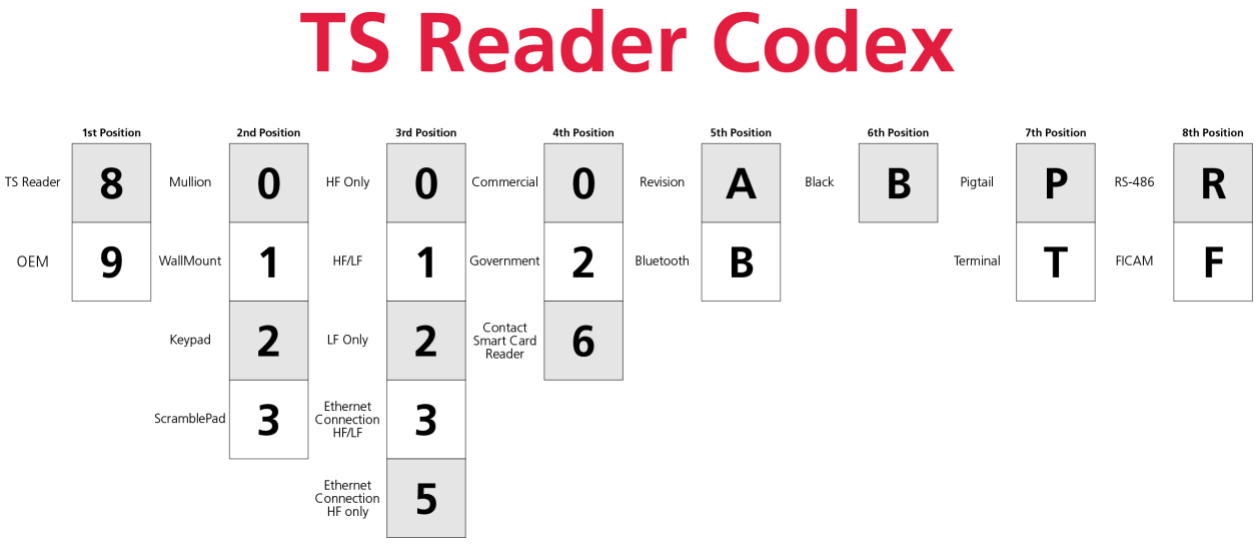
Part numbers are assigned by the Identiv team and will be communicated to the customer before placing an order.

TS Reader Part Numbers

All standard TS Reader part numbers are formatted this way:

- 8XXXABXX000

Please use the following matrix as a reference for determining Identiv’s TS Readers part numbers:



Additional reader options are possible, such as custom LED lighting. Please contact your Identv Sales Representative and/or Philip Fanara at pfanara@identiv.com for those options.

For the VIP Program, custom TS Reader part numbers will be generated at the time of placing an order. The Identiv Team will confirm the exact part number for ordering.

To inquire about this program and pricing, please contact your Identiv Sales Representative and/or Stephane Ardiley at sardiley@identiv.com.