

TWN4

Google Pay Smart Tap User Guide

DocRev2, February 20, 2025



ELATEC GmbH

Contents

| | | |
|-----|---|---|
| 1 | Introduction | 3 |
| 2 | First Steps | 4 |
| 2.1 | Add Smart Tap To Your Project | 4 |
| 2.2 | Configure Smart Tap | 5 |
| 3 | Security Considerations | 6 |
| 3.1 | Key Rotation | 6 |
| 4 | Disclaimer | 7 |

1 Introduction

This document shows how users can enable TWN4 to read Google Wallet Smart Tap passes via NFC connection from a mobile device. In order to do this, Elatec offers a rich toolset for creating a configuration that can run directly on the readers and that returns the pass data payload for further processing. Such configuration can easily be created using the tool AppBlaster which incorporates an integration for adding Smart Tap support. Within this document, only the Smart Tap specific information is handled, please refer to AppBlaster User Guide for detailed information regarding AppBlaster.

2 First Steps

2.1 Add Smart Tap To Your Project

Start AppBlaster, choose "Configurable Project" and select a firmware template your project shall be based on. Next, under "Transponder Types", select "Solutions" from the list "Category" and then select "Google Pay Smart Tap" from the list "Type". In order to complete this step, click the "Add"-button. You will then find Smart Tap in the list "Active Transponder Types".

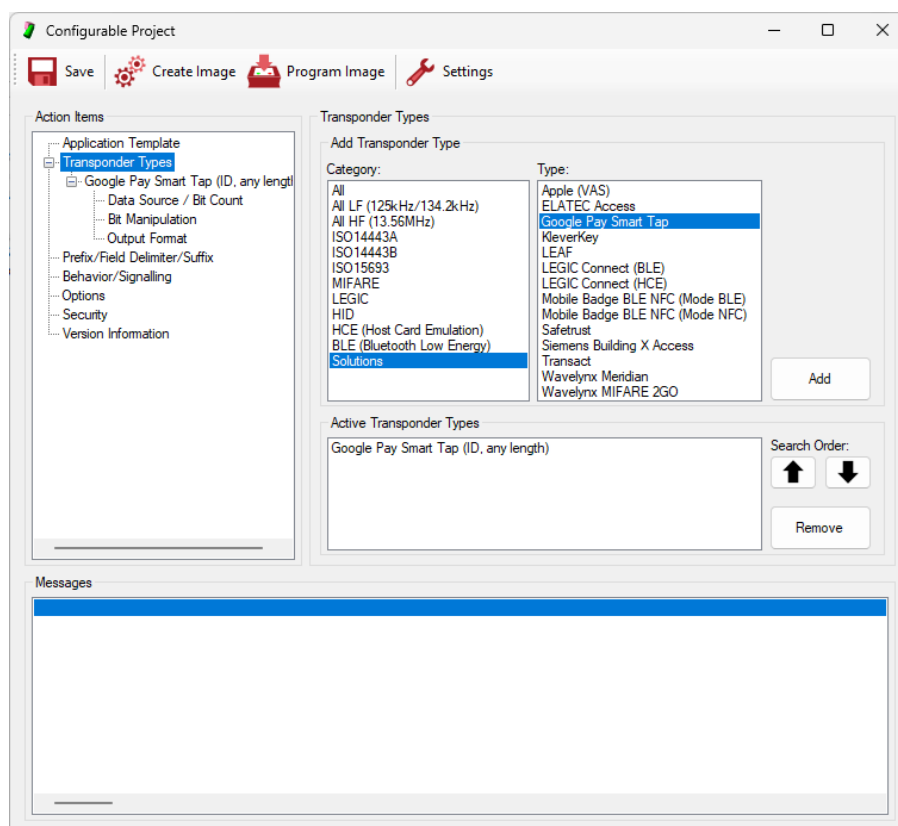


Figure 2.1: Add Smart Tap as transponder type

2.2 Configure Smart Tap

A typical Smart Tap configuration needs the following login credentials to get access a Smart Tap pass:

- Collector ID: A decimal number that must match to the one used in the passes of your project
- Private Key: A 256 bit Elliptic Curve private key, represented as 32 hex bytes
- Long Term Key Version: The version of the entered key, represented as 4 hex bytes

In order to enter the login credentials, select entry "Google Pay Smart Tap" from the list "Action Items". Enter the login credentials into the respective fields. If you want to test a Elatec Demo Pass, you may click the "Elatec Values" button, this automatically sets the necessary credentials. Once this step is completed you may adjust the output format or leave it at default which is hexadecimal output. You can then start test reading of the Smart Tap pass, in order to do this, click buttons "Create Image" and then "Program Image".

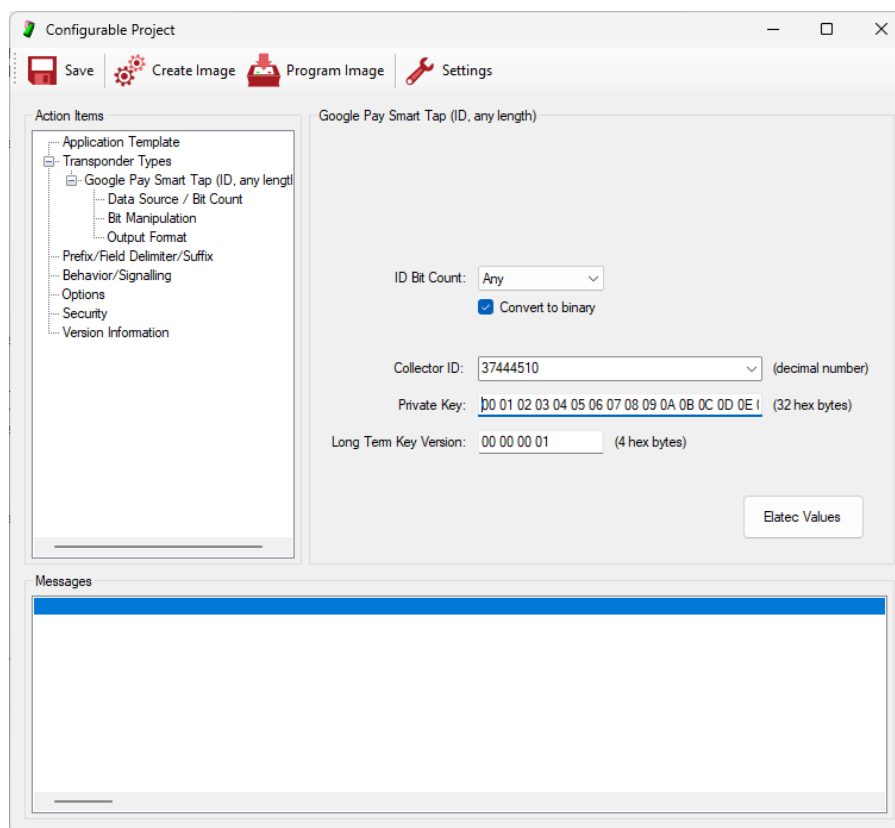


Figure 2.2: Configure Smart Tap Login Credentials

3 Security Considerations

It's necessary to provide an update mechanism of key material in case a key has been compromised. The minimum required key rotation frequency is monthly, but depending on individual security requirements it's recommended to have shorter key rotation intervals. The concrete key exchange strategy is out of scope of Elatec, for more details please refer to the chapter "Key Management" of Google Pay Smart Tap online documentation.

3.1 Key Rotation

Only the private key which is currently in use is allowed be stored on the reader. Any other private key that shall be rotated in as new key shall be stored outside of the reader. In case a key shall be rotated, it's necessary to create an updated configuration which incorporates the new key. This configuration can then be used to update the readers with the new version of the key. The update process can be done by:

- Firmware update directly by AppBlaster
- Remote firmware update if the reader is connected to a network
- Update via RFID Config Card

4 Disclaimer

ELATEC GmbH reserves the right to change any information or data in this document without prior notice. The distribution and the update of this document is not controlled. ELATEC GmbH declines all responsibility for the use of product with any other specifications but the ones mentioned above. Any additional requirement for a specific custom application has to be validated by the customer himself at his own responsibility. Where application information is given, it is only advisory and does not form part of the specification.

All referenced brands, product names, service names and trademarks mentioned in this document are the property of their respective owners.