CD21-Flash-Rev32

Data brief

Flash-memory-based secure microcontroller compliant with the Calypso® specification Revision 3 Version 3.2

Product status link
CD21-Flash-Rev32

Features

- 80 nm Flash memory technology
- Up to 40 Kbytes of user non-volatile memory (NVM)
- Transport application certifications:
  - Calypso Prime
  - Smart Ticketing Alliance according to the CEN/TS 16794 standard

Platform

- Native operating system
- Single or multiple ticketing application

Hardware

- ST31 product based on a 32-bit Arm® SecurCore® SC000™ RISC core
- Advanced 80 nm Flash technology
- Best-in-class RF performance
- Up to 40 Kbytes of user NVM
- Full transaction duration, including typical terminal processing compliant with public transportation requirements
- Common Criteria evaluation assurance level EAL5+

Standard

- Calypso® standard compliant with:
  - Calypso Specification Revision 3 – Portable Object Application Version 3.2
  - Calypso functional specification Revision 2 – Card Application
  - CD97 specifications
  - CD97-BX specifications
  - CD Light specifications

Applications

- Automatic fare collection
- Public transportation
- Access control
- Ticketing payment
- City services and events
- Leisure parks and stadiums
- Corporate cards and student cards

1 Description

The CD21-Flash-Rev32 device is a cost-effective, dual-interface (contact and contactless) secure microcontroller based on a 32-bit Arm® SecurCore® SC000™ RISC core. It is specifically designed for public transport applications, in that it provides a high level of security, high speed transactions and easy evolution capability for transport and multi-service applications.

The CD21-Flash-Rev32 device is available with 8, 18 or 40 Kbytes of user memory.

Note: Arm is a registered trademark of Arm Limited (or its subsidiaries) in the US and/or elsewhere.

1.1 High security features

The security of the CD21-Flash-Rev32 device is managed with various access modes: Pin, Session, Always, and Never.

The cryptographic certificate of the device controls the access to file modifications. The reader (using its built-in SAM) and the card compute this certificate during the transaction, using data encryption standard (DES), DESX (extended DES) or triple DES (TDES) encryption.

The CD21-Flash-Rev32 device implements the Calypso automatic recovery mechanism, which ensures that when data are modified in the card during a secure session, either all the modifications are completed successfully or the data are not modified at all.

The CD21-Flash-Rev32 device provides powerful multi-application synchronization capability: a special mechanism synchronizes modifications between the different applications that the card manages. Each command within the session uses its own secrets, or delegates its security to the session security manager.

1.2 Memory organization

The user memory of the CD21-Flash-Rev32 has the following functionality:

- Multi-application card capability
- Data organized in files in accordance with ISO/IEC 7816-4
- E-ticketing compliant with the EN 1545 standard data model
- The file structure may be chosen among many options (for example, two Calypso applications, one multi-purpose application with nine contracts and one e-ticket application)
- Complete CD Light and CD97 (BX) emulation possible
- Diversified keys protect the data (up to 6 keys per directory)

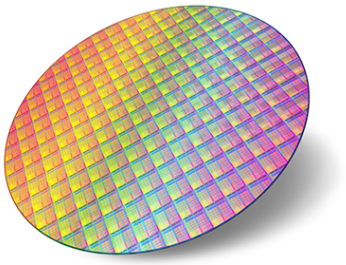
1.3 Certifications

The CD21-Flash-Rev32 device is based on a hardware chip that has the Common Criteria EAL5+ certification. The device itself is certified as a Calypso Portable Object (PO) compliant with the Calypso Prime specifications Revision 3 Version 3.2.

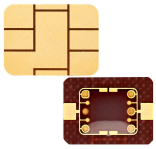
The CD21-Flash-Rev32 device has also obtained the Smart Ticketing Alliance (STA) CEN/TS 16794 certification.

1.4 Delivery forms

The CD21-Flash-Rev32 device is delivered as sawn wafers and in D76 or D78 micromodules.



Sawn wafer



D76/D78 micromodules

Revision history

Table 1. **Document revision history**

Date	Version	Changes
16-Feb-2021	1	Initial release.