



How to migrate your contactless tickets to Calypso

Calypso specifications are based on open standards available to all.

They are designed to facilitate more agile, sustainable and secure ticketing.

Over 170 cities worldwide have already decided to master their ticketing system with Calypso, which frees them from proprietary control.

Moving to occasional use contactless tickets with Calypso is easy. Here's what you need to do...

Calypso Prime enables flexible ticketing across apps and platforms, including smartphones, and is designed to facilitate both interoperability and ABT.

Calypso Light is focused on cost-efficient contactless tickets for transport, events and access control.

Calypso Basic delivers contactless tickets with the same security level as Calypso Prime and Light.

Card commands are parameterized in a single way across Prime, Light and Basic, enabling you to manage a secure session for reading and writing data for all three ticketing offers.*

Ensure you meet the minimum requirements.

You must have:

1. **A TDES key set** (Triple Data Encryption Standard) deployed in your ticketing terminals, to establish cryptographic data protection against security risks
2. **Calypso processing with the APDU (Application Protocol Data Unit) command set**, to enable communication between the card and the reader. This has been part of Calypso since the 2009 specification Revision 3.1, now known as Prime Regular.

Additional recommendations:

1. TDES keys deployed in ticketing equipment to support Calypso Prime card upgrades can also be used for Light or Basic products
2. If several deployed TDES key sets are available, wherever possible, assign one of these sets exclusively to Basic products

Calypso **Prime** and **Light** are based on chips with a security resistance level equivalent to or higher than CC EAL4+ (Common Criteria Evaluation Assurance Level 4+).

Calypso **Basic**, however, is either based on a platform (chip + card OS) that achieves a security certification (CC EAL2+) or on chips that are CC EAL4+ certified. This is why CNA recommends isolating TDES key sets where possible.

Card Pre-Personalization (CPP):

Encode cards with essential data, including security keys

Calypso® basic

Use our free, open source configuration tool to turn your unconfigured SAM into a SAM-CPP-Basic. This means you can accept highly secure Calypso Basic cards across your terminal infrastructure.

Transfer diversified key sets in plain text in a secure environment: this means you do not need a new key ceremony (where keys are created) when the Master SAM (SAM-SP) already has a TDES key set.

CNA members can also access a free tool that will initialize Basic cards with AIDs (Application Identifiers) and network-specific diversified keys, to help identify and secure the cards on each network.

Calypso® LIGHT

Calypso Light shares Calypso Prime's pre-personalisation process to load security keys.

[Find out more](#)

*Please note: while Prime Regular (REV3) products still support backward compatibility with the REV1 and REV2 cards from the early 2000s, these backward compatibility options are no longer supported by Light and Basic.