GEMINI 2000

CONTACTLESS EMV PAYMENTS

STARTER GUIDE

- Introduction
- Hardware
- Software
- Integration
- Certification
- Support

INTRODUCTION

Gemini 2000 is a specialist developer and manufacturer of contactless readers based in Dorset, United Kingdom. For over 20 years, we've helped businesses large and small implement seamless contactless card acceptance into point-of-sale (POS) devices of all types. These include ticket machines, vending machines, electric vehicle chargers, kiosks, product dispensers, barriers, jukeboxes, and more.

This guide is a non-technical introduction to our hardware and software solutions, the type of development work required for integration and the certification process.

The assumed scenario is one where the client builds a proprietary payment solution using our EMV Level 1 and 2 and PCI certified payment readers. Although a significant technical project, building your own solution delivers control, flexibility and cost-savings. Alternatively, off-the-shelf systems are available from our third-party partners.

Is contactless right for you?

Contactless is ideal for fast, low-value payments at attended and unattended point-of-sale devices. It is a secure, convenient payment method that cuts queues and improves user experience.

Contactless readers do not offer PIN entry and transaction values are limited to the contactless card limit. This is currently £45 in the UK.

Our readers are not standalone devices and require integration with your POS device, a back office and a live Internet connection.

How easy is it to deploy?

The ease and speed of setting up contactless depend on the approach to integration. The three main options are outlined on page 4.

In most cases, we offer certified modules for customers with technical expertise to build their own payment systems. It is that expertise that determines the time to completion. We offer consultancy and support throughout all lifecycle stages.

See page 13 for an example of the kind of work required to complete an integration project.

PAYMENT SYSTEMS

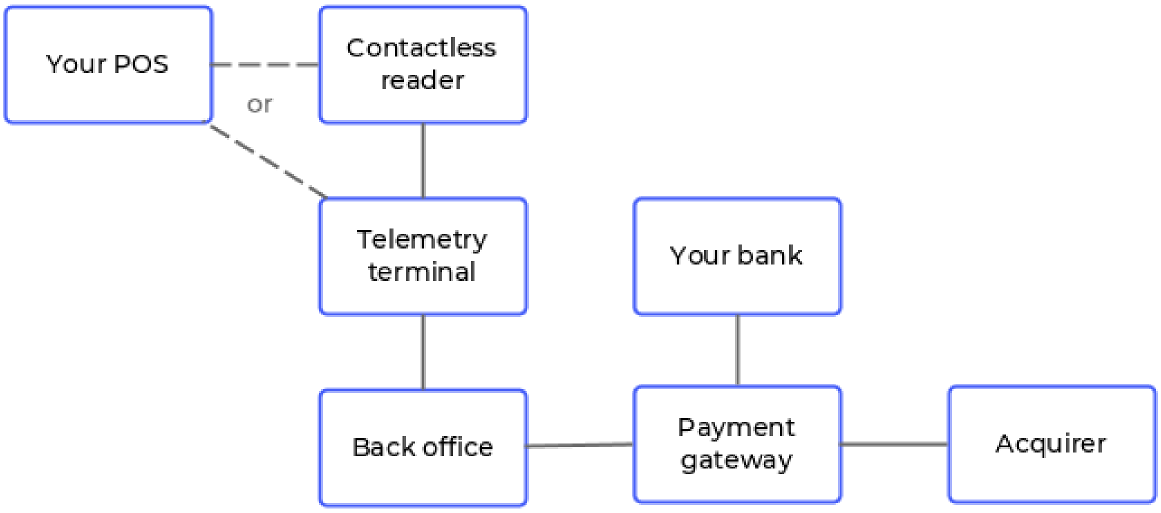
The journey of a contactless transaction

Payment processing systems are typically made of several modules that can be grouped into three blocks:

1. A customer facing POS and contactless reader.
2. A local host (a POS computer or a telemetry terminal.)
3. A financial back office.

Your POS is the beginning of the transaction journey: it sends transaction requests to the reader directly or via a telemetry terminal. The customer is prompted to tap a bank card and the card data is read and encrypted by the reader for secure transmission over the Internet to a back office.

The back office redirects the transaction details to the chosen payment gateway and acquirer for verification. The gateway responds with an Accept or Decline message. This is sent back up the chain to the reader and your POS.



To start accepting payments, you need to take care of all system components: buy certified reader hardware, build your own back office and integrate it with a payment gateway.

Three ways to adopt contactless with Gemini

As OEM manufactures, we offer the opportunity to pick and mix modules for your project. The three most common approaches to integration are outlined below.

	Option 1	Option 2	Option 3
	READER ONLY	**READER + TELEMETRY**	**COMPLETE SOLUTION** ***from our partners***
What is on offer?	Get only the reader and integrate with your Linux, Windows or Android POS or telemetry terminal.	Get the reader and telemetry terminal bundle, and connect to your POS.	Hardware and software bundle that is ready to accept payments out of the box.
Certification	Reader comes Level 1 and 2 certified. You obtain Level 3.	Reader comes Level 1 and 2 certified. You obtain Level 3.	Pre-certified to EMV Level 1, 2 and 3.
Ease of POS integration	Detailed EMV expertise required to integrate our low-level SDK.	Some EMV expertise required to connect our telemetry terminal to your POS.	Easy-to-use API to connect to your POS.
Ease of banking integration	You develop the banking relationships and integration.	You develop the banking relationships and integration.	Banking relationship already set up.
Typical time to deployment	6 to 9 months	3 to 6 months	1 week
Flexibility	The entire system is under your control.	Most of the system is under your control.	You adopt the supplier`s approach, though customisations are often possible.
Cost	Low upfront.	Medium upfront.	Medium upfront cost + a low ongoing charge.

HARDWARE

Did you know…

A contactless reader has to pass over 3,000 tests by accredited labs to gain the certification required by the payment industry. Each uCrypto reader is made up of 174 components, 40,000 lines of code and all the care and expertise of our team. As the visible face of the payment system, the reader is built to meet the demands of frequent use, day after day, year after year.

uCrypto reader is available in a flush mount case, surface mount case, or as an OEM module.

Choosing the right reader

When specifying your hardware requirements, there are three key considerations – the options we make available are as follows:

Mechanical fit

- Flush case
- Surface case
- OEM module

Reader interface

- USB
- Serial RS232
- Serial logic levels

Internet connection

- from your POS
- Ethernet *
- WiFi *
- 4G *

** requires the optional telemetry terminal*

Key features

uCrypto contactless reader:

- Visa and Mastercard certified
- Read cards, phones & wearables
- Accept non-payment cards such as Mifare, DESFire, NTAG.
- USB or Serial interface
- PCI PTS v5.1 certified option
- OLED display option
- Spare SAM slot option

Telemetry terminal:

- A separate optional box to host the business logic
- Open Linux platform
- Ethernet wired connectivity
- WiFi or 4G wireless connectivity
- Ready for EMV Level 3
- Optional MDB/Pulse communication module

Before you buy – your hardware integration checklist

Will the reader fit into your POS and work as expected? This checklist outlines the key considerations to make when deciding on installing a reader.

☐ Size. Check that the reader fits mechanically – dimensions are provided below.

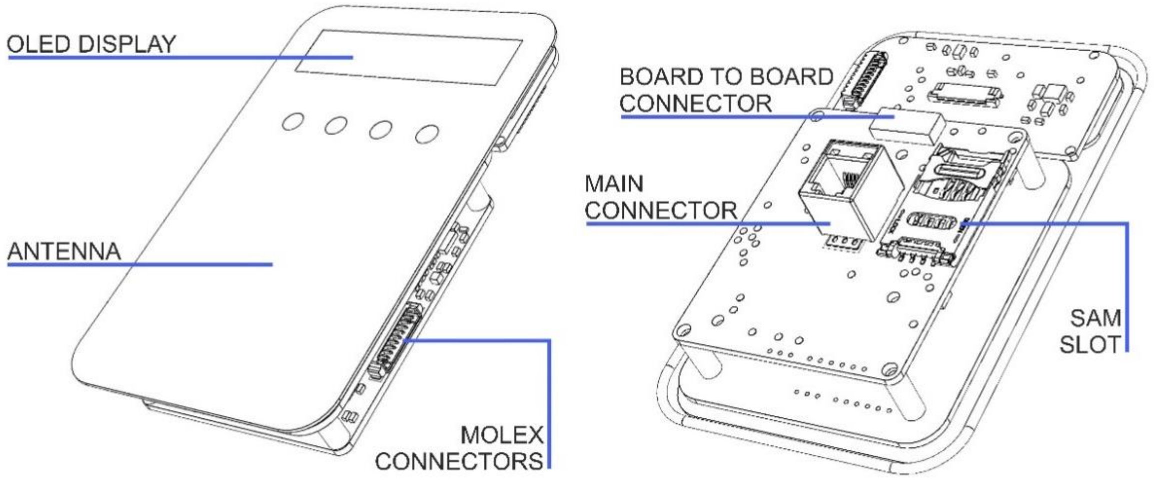
☐ Radio interference. Ensure there are no metal objects, for example metal housing parts, within 2cm of the reader antenna.

☐ Thermals. The reader should not be installed near excessive heat sources and kept within its stated operating temperature range at all times.

☐ Power supply. 5V 2A is required for the reader or 12V for the telemetry terminal.

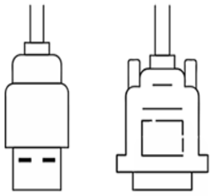
Inside the reader

uCrypto consists of a main board and antenna board sandwich housed in a tough plastic case. An optional display is available. The main connector is an RJ12 (for either USB or Serial connection) or you can opt for Molex or board to board connectors.



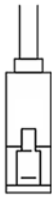
Cabling

uCrypto cable options include USB Type A or Serial 9-Way D-sub connectors. Custom cable lengths or other connectors can be provided upon request.



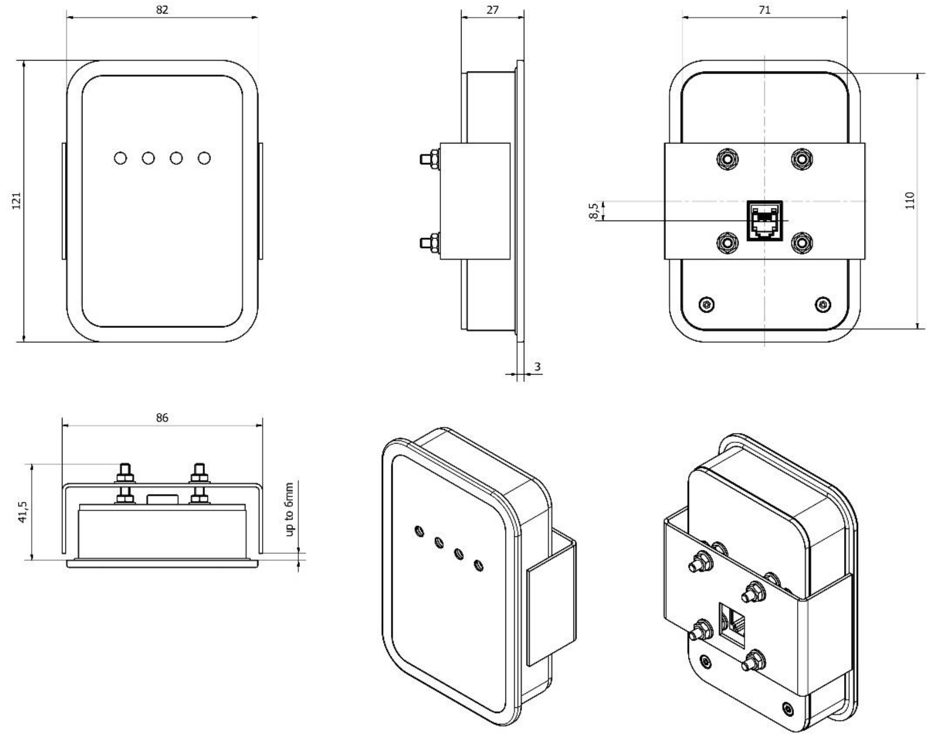
The telemetry terminal provides Ethernet connectivity via an RJ45 port for standard cat5 network cables.

WiFi and 4G are also available.

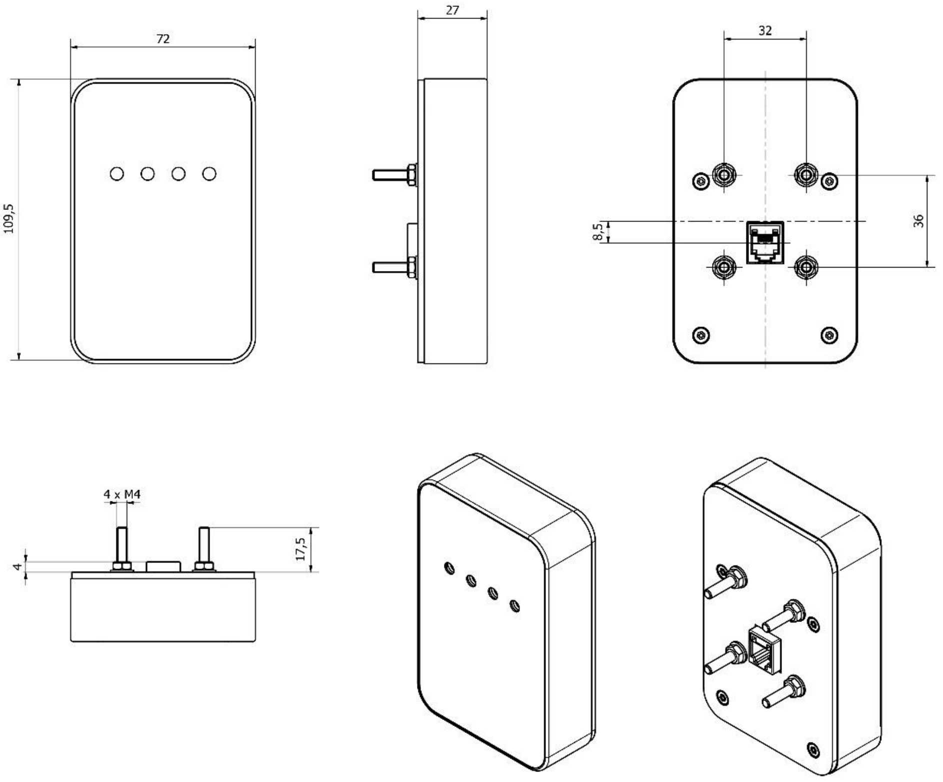


Contactless reader casings

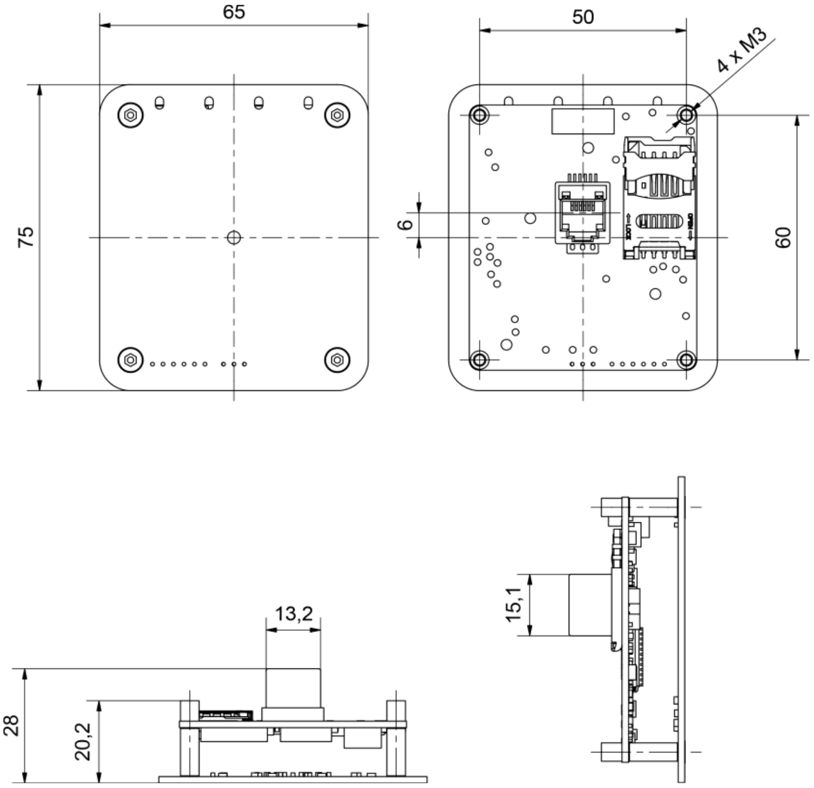
Flush mount – shown with a U-shaped holder bracket.



Raised mount – for surface installation.

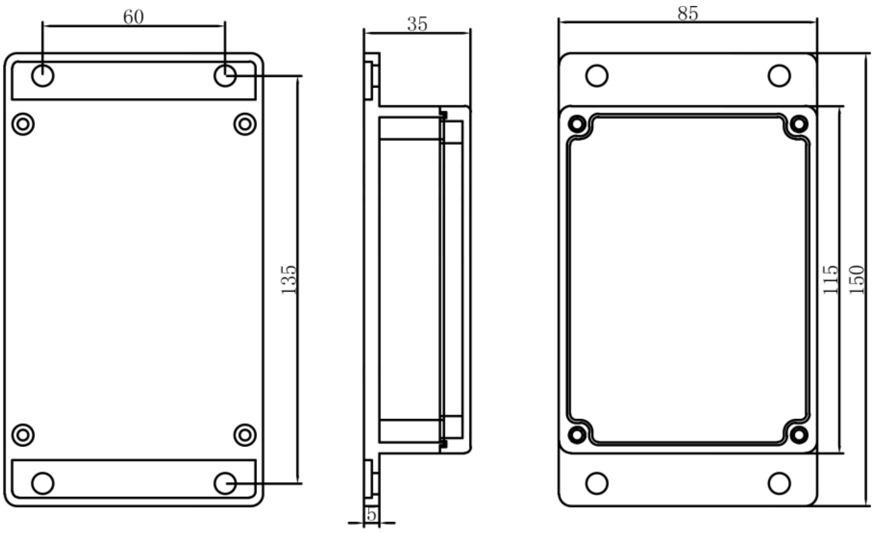


OEM module for installing inside your enclosure. This is possible when a 3mm thick non-metal front cover is used. EMV re-certification requirements may apply.



Telemetry terminal casing

The terminal connects to the reader via a cable slotting into a locking RJ12 connector. When using 4G additional space is needed at the top for an antenna.



Reader specifications

Physical specifications

Dimensions	65x 75 x 28 mm (OEM module)
Weight Approx.	40 g (OEM module)
Status Indicators	Beeper 4 LED indicators 1 health-check LED

System

MCU	Kinetis K81
Operating System	FreeRTOS
Clock rate	150MHz

Contactless interface

Operating Frequency	13.56 MHz
Chipset	PN5180
Communication Standards	ISO/IEC 14443 (Type A & B) NFC ISO/IEC 18092
Card Reading Distance	Up to 70mm
Transmission Speed	Up to 848Kbps

Contact interfaces

Card Slots	One spare SAM card slot Expansion boards available

Connectivity

Host Interface	RS232, Serial UART, USB CDC

Power Supply	5V DC
Current Consumption	350mA@5V peak

Security

Cryptography: DES/3DES, AES, RSA, SHA-1, SHA-256

EMV certification

EMV Level 1
EMV Level 2 Visa and Mastercard
TQM Label

Application interface

Supported APIs	G2K API Crypto Interface API

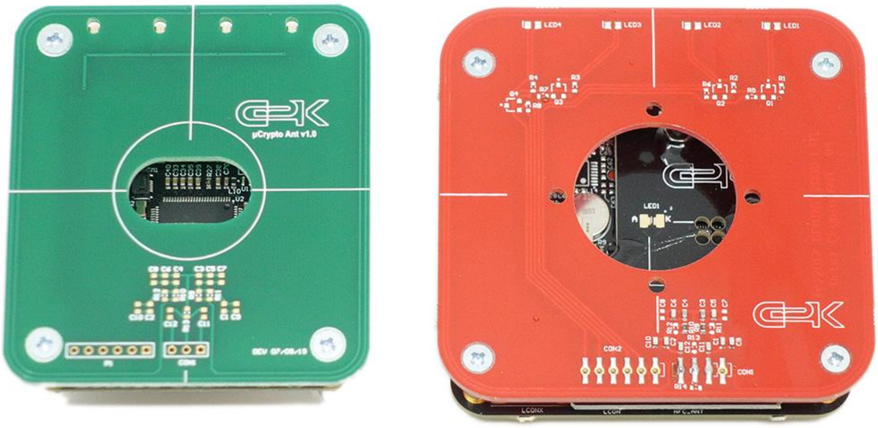
Operating conditions

Operating Temperature	-25 to +80 °C
Non-Operating Temperature	-40 to +85 °C
Operating Humidity	0–95% non-condensing
MTBF	500,000 hours

Differences between Crypto and uCrypto

This guide details the uCrypto reader, but a bigger reader called Crypto is also available. Crypto is a more specialist device aimed at transit applications. It has a larger form factor than uCrypto, supports RS485 and SPI interfaces (not available on uCrypto) and a choice of 12V and 5V power supply (only 5V on uCrypto.) Crypto has no casing options and is available as an OEM module only.

Both readers share the same firmware.



uCrypto and Crypto OEM reader modules

Getting a hardware quote

We understand that price is an important consideration for most projects. We aim to offer competitive, straightforward pricing – contact us now to get a quote. Price breaks are available for larger volumes, and opting for different hardware features.

About our manufacturing process

We have been designing and manufacturing readers in our own facilities since 1997. Our processes and production facility are certified to ISO 9001 and Mastercard's Terminal Quality Management scheme. We are dedicated to continual improvement, quality control and configuration management – and working hand in hand with clients to deliver best-in-class solutions.

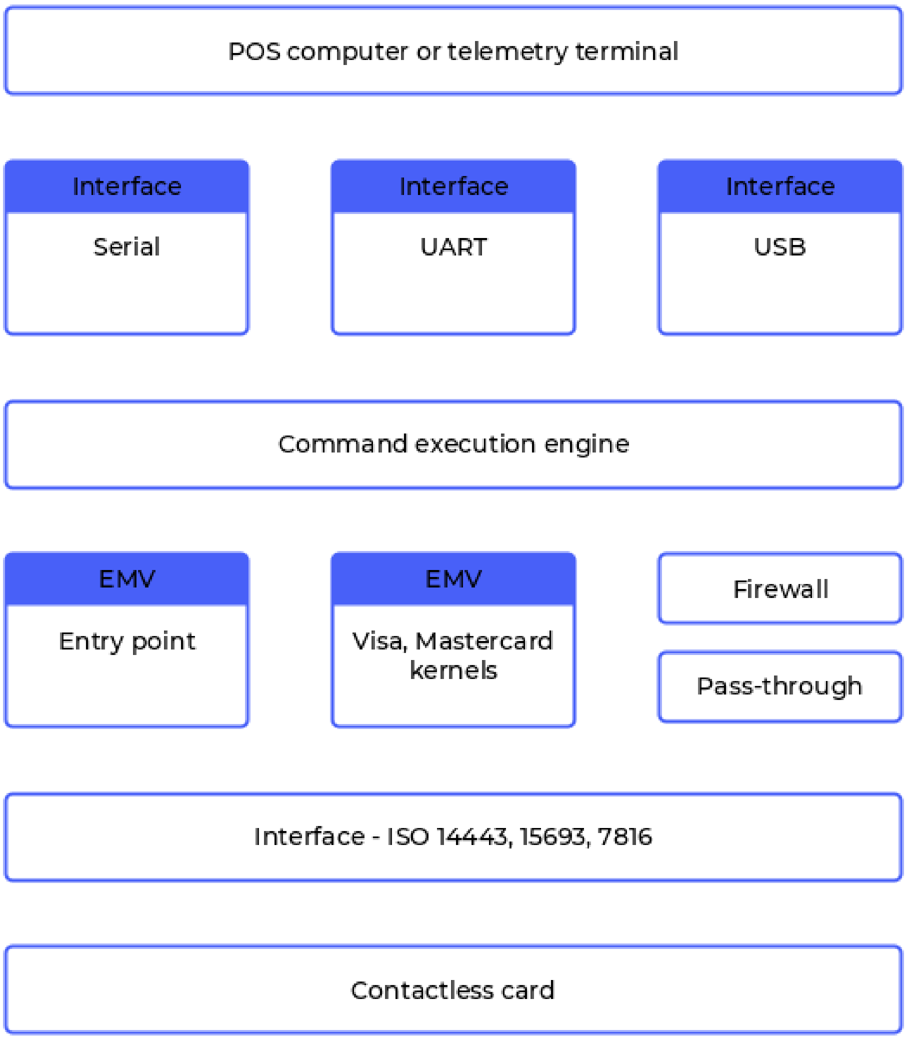
SOFTWARE

Reader firmware

Crypto is a family of contactless payment modules that shares the same EMV-certified firmware. There is no file system or operating system, which means that the reader can be shut down instantly without corruption of keys or losing configurations; power up is also fast.

The reader communicates via serial interface – RS232 or UART logic levels, or USB CDC. The host (POS computer or telemetry terminal) sends commands and the reader returns result code and data. The host always initiates communication first. Communication with the host is carried by a proprietary Block Framing Protocol.

The functional blocks of the Crypto firmware are shown below:



Open and closed loop support

The main advantage of Crypto is the clear split between open loop and closed loop applications. All EMV payment (open loop) modules within the firmware are certified by EMVCo, Visa and Mastercard. Closed loop schemes, for example reading of Mifare cards or the transport schemes ITSO and Calypso, are executed by the host via the reader's Pass-through mode.

As the host computer is usually a comparatively high-performance device, non EMV apps that run on it benefit from its powerful processor.

Security, simplified

Crypto is a highly secure payments module: it incorporates a cryptographic engine and secure key storage as required by the Payment Card Industry, and is certified to PCI PTS POI v5.1. It does not allow any arbitrary code to run in the firmware. Its firewall protects cardholder data and security keys from unauthorised access by closed loop applications.

As a result of this design, the host and other systems are completely outside of the PCI PTS scope, which makes PCI DSS and P2PE schemes easier to certify.

Getting started with the API

The API implements the reader's Block Framing Protocol and takes care of the low-level communication layer. All available commands are identified by a command code. Each command takes a number of parameters and returns a result code, and any data when available.

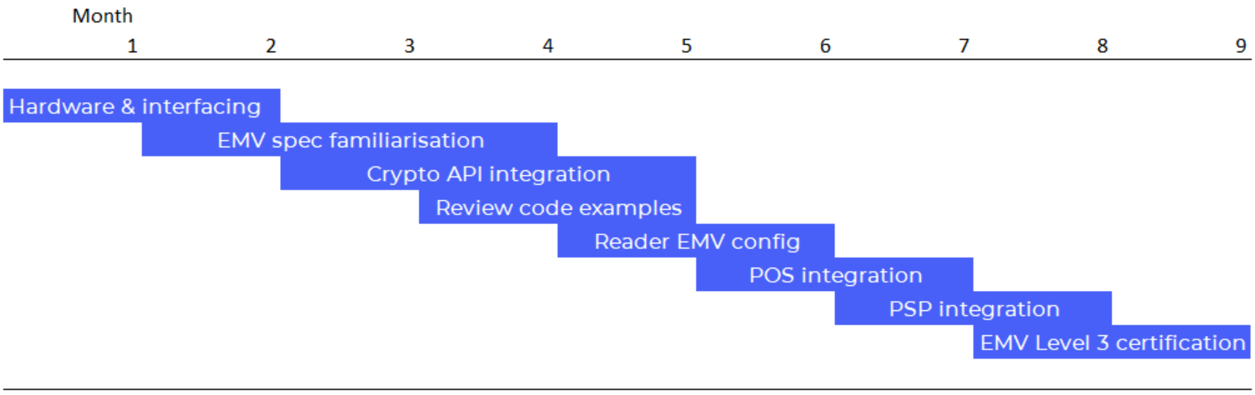
All commands are accessible via the API library. An additional library – Crypto Interface library – is provided to facilitate EMV contactless payment transactions. For more details, please refer to Crypto Interface Library User Manual.

For detailed software development documentation refer to Gemini 2000 API4.0 Reference Guide and Crypto Developer Guide.

The Crypto programmer must be familiar with BER TLV data formatting and EMV Contactless payment concepts including VISA and Mastercard specifics.

A typical integration project

No two projects are alike, but some tasks are common to all. Below is an example of the kind of work required to build and deploy a payment system based on the Crypto contactless reader. Customers typically take 6 to 9 months to completion.



Hardware and interfacing

Choose the reader hardware for your project and establish USB or Serial communication with your POS.

The EMV specification

Understanding the EMV payment specification in detail is key. We'll point to reference documentation to use.

Crypto API integration

Connect to the reader through the API and interface libraries on Windows, Linux or Android.

Code examples

We provide a basic payment terminal application project that you're welcome to study as a basis for your own system development.

EMV configurations

Each business case requires different configurations for the reader, as per EMV specifications. These also need to be defined for different Level 3 tests.

POS integration

Build your POS logic and generate transaction requests for the reader.

PSP integration

Exchange transaction data from the reader with your financial partner for processing and approval.

Level 3 certification

Your financial partner will test the entire payment system. When all tests are passed, a Level 3 certificate is issued that lets you go live.

Remote management

With ever-changing functional, regulatory and security requirements, over-the-air update is a must for any new payment reader. Crypto has capabilities for remote key management as well as firmware updates. The NFC front end is firmware upgradeable, so new EMV Level 1 and 2 requirements can be implemented.

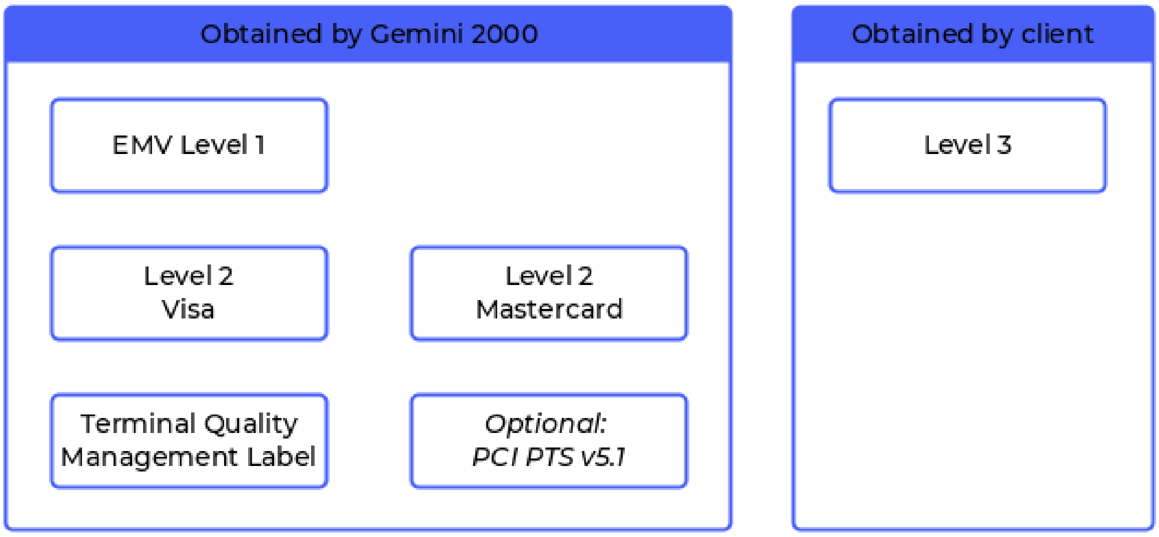
All updates are possible through a Terminal Management System, either built by the customer or provided by Gemini 2000.

CERTIFICATION

Certification in a nutshell

The payment services industry sets strict standards to ensure the security, robustness and interoperability of hardware and software modules. These are enforced via a certification process managed by accredited labs. Crypto readers come with most required approvals already in place, such as EMV Level 1 and 2.

Our customers need to complete Level 3 certification only, which involves passing tests on the final payment system against applicable payment scenarios.



Do hardware and software changes invalidate certificates?

Certificates are issued for a given state – model and version number – of a payment module. Any changes, for example in the physical casing or firmware functionality, must be evaluated in order to determine whether the certificates are still valid.

Changes are classed as major or minor, with the latter being deemed acceptable by approval bodies for deployment without recertification.

Certificate glossary

Level 1

Managed by EMVCo, this certificate is issued after testing the physical reader hardware, its radio capabilities and card communication. For example, tests are made with reference cards placed at pre-defined positions near the antenna. There are also analogue tests around the target frequency and digital tests on the low-level communication protocol.

Level 2

Tests around the payment application selection and financial transaction processing for each card brand such as Visa and Mastercard (each known as software “kernels”.)

Level 3

Card brands are tested against the entire processing solution, from the reader to communications with the acquirer. Level 3 requires that the terminal is complete with its EMVCo-approved hardware, software kernels, and payment application in place, and must be connected to a test environment.

PCI PTS

This is a security related certificate issued by the Payment Card Industry (PCI) Security Standards Council. It involves in-depth analysis of the reader security and attacks performed in a lab to find any vulnerabilities. PTS stands for PIN Transaction Security, which does apply to Crypto (a contactless-only reader with no PIN entry capability) through the programme’s Secure Reading and Exchange of Data (SRED) module. Crypto has a secure version certified to PCI PTS SRED v5.1.

Not all applications require PCI PTS. Get in touch to discuss the pros and cons.

Terminal Quality Management (TQM)

This programme was created by Mastercard to ensure that the functionality of contactless readers, as certified during type approval testing, can be sustained throughout the manufacturing cycle. Production processes are reviewed on-site at the factory to ensure good quality control and configuration management.

WORKING WITH US

How Gemini is different

We aim to be more than a supplier to our customers and work to forge long-lasting partnerships. We believe our true added value is in:

- Sharing of expertise. We rely on our experience with contactless payments to provide technical consultancy and help you design and launch your project.
- Customisation. We can make changes to deliver a solution tailored to your project needs. Ask us about co-branding, custom cabling, mechanical changes or software upgrades.
- Assisted integration. Getting a payment project off the ground can be a significant challenge. Our hardware and software engineers are on hand to help you through development, testing and deployment.
- Technical support. We're here for everything that happens after launch, be it maintenance, upgrades or bug fixes.

Getting in touch

You can reach us on:

info@gemini2k.com	+44 (0)1202 666 700

To get you started with evaluating our products, we can provide documentation, pricing, samples and consultancy.

In order to find out whether Crypto is right for you, we typically first ask:

- What is your existing POS hardware and software that will be upgraded to contactless payment acceptance?
- How do you see the contactless reader fitting mechanically?
- Whether you have preferred banking partners already?