White Paper

CmDongle with Flash Memory in Practice

Oliver Winzenried, CEO Wibu-Systems
www.wibu.com

WIBU SYSTEMS

Content

Author:

Oliver Winzenried is a security enthusiast with a vocation to expand universal knowledge and apply innovative technologies to protect the intellectual property and business revenues of ISVs. With a degree in Electrical Engineering from the University in Karlsruhe, he began his entrepreneurial career immediately after completing his studies, and focused on electronic and ASIC design, hardware, microcontroller and embedded application development for consumer electronics, automotive and industrial engineering. With Marcellus Buchheit at his side, he then founded Wibu-Systems in 1989, and remains the company's CEO. His passion for software protection has resulted in numerous patents covering areas from secure license management and anti-tampering solutions to dongle feature innovations. He's also a prolific author, greatly contributing to editorials and books on the one hand, as well as addressing large audiences at trade shows, conferences, industry associations and technology centers like the Fraunhofer Institute. He is personally committed to R&D projects and organizations for standardization, such as the SD Card Association. Oliver Winzenried is also serving as chairman of the Product and Know-how Protection "Protect-Ing" committee of VDMA, member of the board of directors of Bitkom, and member of the managing board of the FZI at KIT. In 2015, he has been elected Manager of the Year in the Automation category by the readers of the German electronics publication Markt&Technik.

Introduction

Wibu-Systems produces software and dongles to protect all types of OEM software. Wibu-Systems' products guarantee the integrity of data, applications, and communication. With versatile, fine-grained licensing methods, new business models become possible for OEMs, and existing business models are protected for the future. Wibu-Systems' technology prevents product piracy and secures the products of software developers, mechanical and plant engineers, and the makers of controllers and other devices from counterfeiting and tampering. CmDongle with integrated flash memory is the strongest integrated protection product. It comes with dedicated data partitions that are ideal for mobile software operators, service technicians, or intelligent device manufacturers. This white paper reviews the areas of use and applications that benefit from the new capabilities of the flash memory-equipped CmDongles.

Why Protect Software?

A Connected World and its Enemies

Illegal counterfeits, reengineering, or illicit copying threaten the invaluable know-how of companies everywhere. This is not a new danger, and other threats, such as sabotage, manipulation, or espionage via malware or wiretapping are a familiar reality. The world has become more connected. The time of isolated solutions has long passed. The connected world has opened new avenues for attacks as machines have begun to communicate via TCP/IP networks. Such networks are not secure – and the Internet is most likely the least secure network of all. A soft underbelly has been exposed to new forms of threats.

Data Integrity and Access Rights

Protection strategies are nowadays required in many places where they would never have been needed before. Reports about hacked cars or medical devices accessed from simple laptops have hit the news and demonstrate how important data security and integrity have become in our daily lives. Hackers cost the economy millions, as the recall of 1.4 million Jeeps by Fiat Chrysler in the United States after a hacker attack has shown. The attack on the car's control systems simply used a mobile phone connection to access the vehicle's entertainment systems.

All in One – Security and Flash Memory

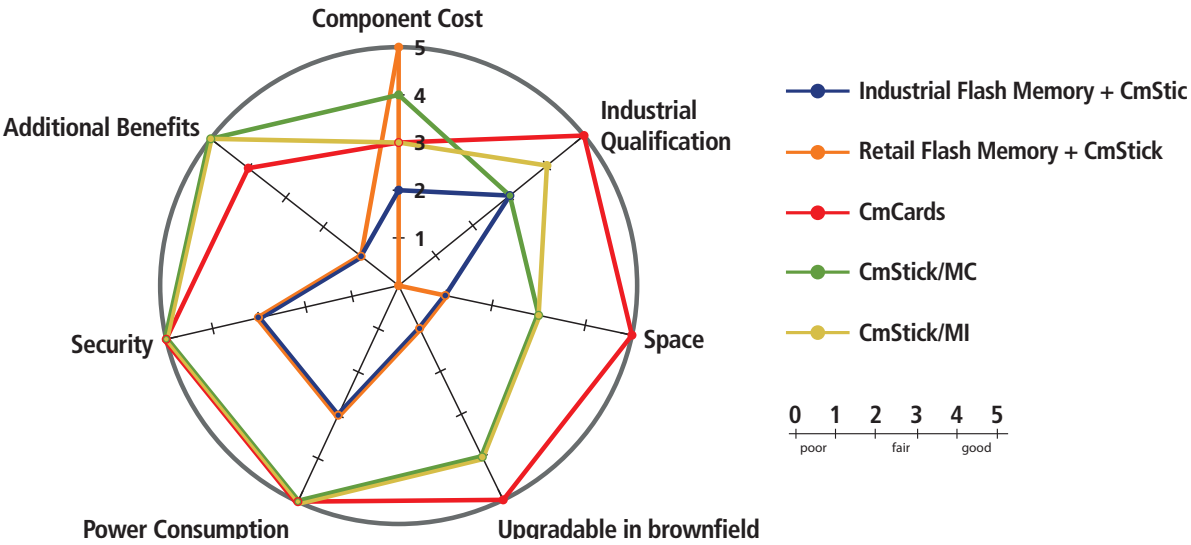
CmDongle with Integrated Flash Memory

The CmDongle with integrated flash memory includes CodeMeter® smart card chip with space for more than 1,000 licenses and the full complement of CodeMeter security functions. The built-in flash memory can be accessed like any disk and includes data partitions in different sizes. Each CmDongle with flash memory comes with a CmPublic partition and a CmSecure partition. The USB stick model also includes a CmPrivate partition and a CmCdRom partition. These four partitions are unique to these highly integrated dongle designs. The partitions can be customized to the user's needs. They allow for new products and design strategies as will be outlined below. The dongle is available as USB stick, microSD card, SD card, CF card, and CFast card. Whatever the form factor, the full CodeMeter security functionality comes built in. This includes symmetric and asymmetric encryption, signatures, and the storage of X.509 certificates. The card products come with SLC flash memory, the industrial-grade USB model with up to 8GB SLC flash memory, while its commercial-grade cousin comes with up to 64GB Samsung eMMC 2-Bit MLC flash memory. CmDongle with flash memory can operate in temperatures from -40°C to +85°C; the SLC flash memory technology offers longest life, low power consumption, memory protection with AES encryption, and long availability in the market. In short: CmDongle is industrial ready!

Six Reasons in Favor of the Combination Product

What makes the combination of flash memory and security technology on one device so special if all security functions of CodeMeter are available without any flash memory at all? What are the benefits of a combination product?

- **Lower costs:** In economic terms, any reduction in the number of components is a reduction in admin costs.
- **Industrial-grade design:** The productivity of devices increases the longevity of its components that operate without errors or outages. CmDongles with flash memory are designed, produced, and prepped for industrial applications. Their long life and long availability reduces the total cost of ownership and increases profits.
- **Space:** The smaller form factor allows the security functions to be included in very small-scale devices.
- **Upgradeability:** The combination product can be used with new software to upgrade the security of existing devices. Devices already in the field can be upgraded without any changes to their hardware, as the standard form factors USB stick, microSD card, SD card, CF card, or CFast card cover the entire range of common mobile flash memory solutions.
- **Versatility:** Four special data partitions offer new opportunities for products and functions. These include the secure storage of highly sensitive data on mobile devices, mobile software solutions, and increased security for the entire solution.
- **Greater security:** The close, built-in combination of smart card chip and flash memory adds to the security of the design. Gambling machines, ATMs, or other devices that are targets for tampering and other attacks can benefit from this unique quality.



Economy Matters: Logistics, Administration, Certification

How much revenue a manufacturer generates with a device can only be known once all costs have been deducted. All costs incurred during the entire life of the device are known as the Total Cost of Ownership (TCO). This includes the simple cost for the components as well as the spending on logistics, administration, certification, repairs and servicing, replacements, training, maintenance or other lifecycle expenditures. In a direct comparison, CmDongles with integrated SLC flash memory disk come at a higher upfront price than other flash memory cards that typically employ MLC flash memory technology. Their economic advantage lies in the reduced need for logistics, administration, and certification. Fewer parts means lower admin costs. A single unit has to be procured, only one item introduced in the ERP system, and only one component stored, monitored, or replaced. Components for industrial applications are typically available for many years in identical formats. Firmware and internal electronics remain unchanged in order to work reliably in all OEM applications. Another advantage is its long life for greater equipment reliability. The dongle comes with a range of certifications to make the full certification of the embedded device easier and cheaper. In a TCO calculation, the higher purchase price becomes a negligible factor.

Made for Industry

Device availability and reliable operations are the prime directive for industrial applications. For integrated flash memory, this means that no data can be lost in case of power outages. Data integrity must be guaranteed even after many accesses. Wibu-Systems has decided to use only SLC flash memory with high-end industrial flash memory controllers made by Hyperstone, Europe's only maker of flash memory controllers. Hyperstone is a specialist for industrial applications; Swissbit makes industrial-grade memory, produced in Germany. Swissbit manufactures the CmCards for Wibu-Systems. It uses Common Criteria certified smart card chips like Infineon's SLx97 with EAL5+ certified hardware and Cryptolib. The electronic components and manufacturing partners are selected with long life, reliable operations, and the constant availability of identical CmDongles with flash memory in mind, supported by specific design decisions. CmDongles have industrial-grade properties and are designed for use in a wide range of temperatures. They can be delivered with Conformal Coating. The MTBF (Mean Time Between Failures) of the CmStick/MI (industrial) with SLC flash memory is over three million hours, that is, more than 350 years. In commercial terms, the costs of machine stoppages or service repairs as a result of faulty memory far exceed the costs of long-life, high-reliability SLC cards. There are certain applications with less stringent requirements and more emphasis on value for price, which can benefit from the CmStick/MC (commercial) with high-quality 2-Bit MLC memory of Samsung's eMMC-2000 series.

Reasons for using SLC Memory

Investment Costs vs. Risks

The life expectancy of a memory card depends on its internal design and technology. There are Multi-Level-Cell-flash memory technologies that can distinguish between two states of the cell, meaning that four or eight different charge states (in the case of the TLC Triple Level Cell) are identified when writing to or reading from the floating gate transistor, compared to the regular two states. A cell can hold more than one bit with this technology. Such Multi-Level-Cells are cheaper, because more bits are available per square inch, but they are more susceptible to disruption. Bit errors and catastrophic failure become more likely. In the end, the life expectancy of the memory shrinks. Processes to correct bit errors become increasingly complex when more than one bit is expressed in each cell.

Designing for Industry vs. Price and Performance

At the chip level, manufacturers need to know which objectives they are pursuing. If the goal is to save costs or achieve high write speeds, as in the case in most consumer-grade flash memory products, durability, MTBF, electric stability, or power consumption are not as important. Since Hyperstone has committed itself to industrial-grade designs, its goals are long-lasting availability, reliability, data integrity after power failures, and power consumption. That requires other resources and intelligent capabilities in the controller. Special firmware manages internal controller functionality, such as early acknowledgement, in an industry-ready manner to ensure that no data is lost when the power supply is disrupted.

Safety Features	Endurance Features		Performance Features	Added Features	
Power Fail Management (patent)	Read Disturb Management	Global & Static Wear Levelling (patent)	Adaptive Read Ahead	SMART	Custom Timings
Redundant Firmware	Dynamic Data Refresh	Bad Block Management (patent)	Configurable & Dynamic Early Acknowledgement	Security	Conditional Access
Error Correction Management (patent pending)	Reliable Write (patent)	Read Retry threshold shifting	Copy Back Management	Sanitize	In Field update

Hyperstone hyReliability™ Flash Memory Management - Overview selective Features

"When using flash memory in industrial applications, our customers require endurance and reliability. Fast SLC memories and flash memory controllers both with long-term availability are key. Hyperstone flash memory controllers match these mission profiles perfectly by offering essential NAND flash memory management features. Ensuring data integrity and prevention of data loss upon power outages are necessary in order to guarantee safe operation of critical machinery." says Steffen Allert, VP Sales Hyperstone.

No Space in Embedded Devices

Many embedded devices are tiny and use every last bit of available space. However, most embedded systems include flash memory storage for applications and other data. If this original flash memory card is replaced with a CmDongle with integrated flash memory, the same form factor and same number of interfaces now comes with maximum security. The smallest version of CmDongle with flash memory comes as a microSD card. At only 11 mm × 15 mm × 0.7 mm in size, it fits even in the tiniest devices – a great opportunity for making the controllers, sensors, and engines of the Industrie 4.0 world more secure.

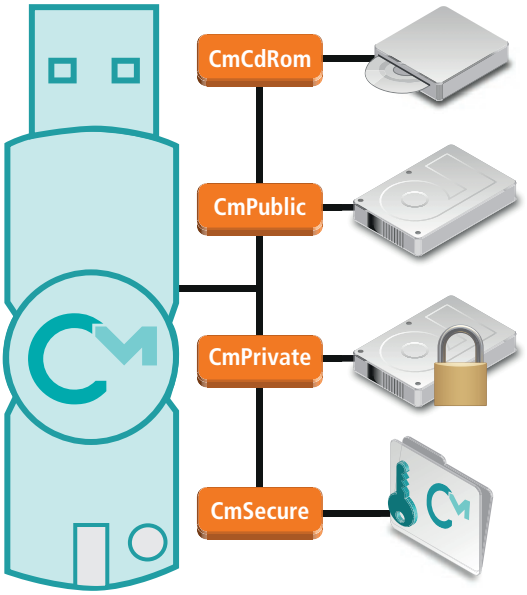
Retrofitting Security

Industry and legislators are responding to the increasing threat of cyber crime with new regulations or changes to old rulebooks. One recent example is the new act on IT security. Technical protection measures are already required by law for medical devices. New devices have begun to include security by design, but many old devices are still in use until they are eventually replaced by newer machines. These can now benefit from the ability to retrofit security technology in an easy and streamlined manner. Security measures can be added whenever normal smart card connections are available. The existing hardware remains untouched, and only the software needs to be adjusted for the new security functions. Little effort is needed to bring old technology up to the newest standards of security.

Four Partitions and an Infinity of New Applications

CmPublic

All CmDongles with flash memory storage come installed with a public partition at maximum size. In the original state, the host can access this partition with full read/write rights like any disk. Adjusting the settings allows the OEM to activate a CmSecure Disk on CmCards and USB CmStick/M. The USB CmStick/M also offers the CD-ROM partition CmCdRom and the secure private partition CmPrivate.



Disk vs. USB HID

The USB CmStick/M can be set for so-called HID-only mode. HID is an acronym for “Human Interface Device” and normally refers to devices like mice or keyboards. The selection determines how CodeMeter hardware and the host system interact with each other. In HID mode, all CodeMeter security functions are available and a CmSecure disk can be created, but the other partitions are not available. The advantage of HID mode is that the host system does not treat CmStick as a USB memory stick, but as an input device. No malware or viruses can be transferred to the system. All CmCards and CmSticks/M with MSD (Mass Storage Device) come with a Codemtr.io file on their CmPublic partitions to enable communication with the smart card chip. A patented communication procedure allows data sent to the smart card chip, where it appears to be stored in a regular file. Instead, the apparent Codemtr.io file is a file I/O that communicates with the smart card controller in the form of read/write commands.

CmSecure

The host system cannot access the Secure Data partition as a regular disk. Data in this partition can only be written or read out in blocks via CodeMeter API used by correctly authorized software. The Secure Data Partition typically holds OEM-specific data, which makes it a major obstacle for hackers and a great security advantage. In the same manner, it can be used to store settings and user rights, or to keep log files protected from tampering. Extremely confidential data can also be stored here for optimum protection from unauthorized access. The data in the Secure Data Partition can, for instance, be used by service technicians for temporary or permanent rights to certain actions. Mobile IT forensics uses the Secure Data Partition to record the findings of forensic investigations in a tamper-proof, forensically viable format.

CmPrivate
The USB stick model also includes the CmPrivate partition for use with sensitive data. It only becomes visible after entering a password or enabling it via the API. The data is stored in AES encrypted form, making it uninteresting for hackers even when they overcome the considerable access restrictions. The partition can also be set as read-only.

CmCdRom
The USB stick model comes with an additional CmCdRom partition which the host system recognizes as a CD drive to write to. However, it cannot delete or overwrite any data in the partition, where applications are typically stored. Mobile applications are launched in a secure environment that leaves no traces on the host system. This is an important property not only for IT forensics specialists but for technicians on maintenance calls who can use diagnostic applications that cannot be used in normal operations. The partition can host a mobile lab or store important documents like user manuals or specifications for ready access without Internet connections.

Applications

Gambling Machines


Gambling machines are exposed to a variety of potential threats as games must not be copied or used in cloned machines. The machines themselves must not be tampered with for illicit gains. Only licensed software from an authorized source must be used on them. The software must be easy to replace without compromising security. A secure storage medium fulfills all of these requirements.

Security-relevant Tasks:
- Software integrity
- Secure boot
- Tamper-proofing
- Licensing
- Protection against reverse engineering

Advantages of the Combination Product:
- Standard smart card format
- CmCdRom partition for game code
- CmSecure partition for licenses and log files
- CodeMeter integrated for all security functions

Service Technicians and ATMs


Automatic bank teller machines are particularly at risk during maintenance. Their security is protected only when authorized personnel get access to the relevant parts for a limited time and predefined tasks. At the same time, service technicians need to have all documents, testing applications, and relevant licenses for functions not yet released with them on site. The ideal solution would have the entire set of user rights, keys, and testing software in a small, handy, and easy-to-use package, while ensuring that its loss or theft represents no major security risk. This is where the CmDongle with flash memory storage in e.g. a USB stick form factor can apply all of its benefits.

Requirements:
- Two-factor authentication with password and dongle
- Ease of use
- A single password for all protected applications
- Individual passwords for each CmDongle and user
- Mixed systems
- Mobile use without network or Internet access
- Time-bound licenses

Advantages of the Combination Product:

- Handy USB stick CmStick/M
- CmCdRom partition for testing applications, user manuals, and wiring diagrams
- CmSecure partition for service protocols
- CmPrivate partition for other confidential data
- CodeMeter integrated for all security functions

Mobile IT Forensics on a USB Stick

IT forensics software is employed for investigations in modern technology. The key is to protect the forensic integrity of the data, which means that neither the suspect's device nor the data on it must be altered. The software needs to be ready for mobile use. Investigators can bring their forensic toolkit on a USB stick and collect their findings and evidence on the same stick.

Requirements:

- Digital evidence that holds up in court
- Protection against cloning or manipulating the forensic software
- Booting and using an operating system without any alterations or installations on the host computer; the target hardware needs to be accessed from a secure environment.
- Software started on the kernel level without need for device drivers
- Secure storage space for any type of data recovered from the target computer.

Advantages of the Combination Product:

- Handy USB stick or CmCard
- Boot partition with forensics software
- CmPrivate partition for recovered data
- CmSecure partition for log files
- CodeMeter integrated for all security functions

Embedded Systems, Controllers, and Field Devices

Internet of Things (IoT) and Industrie 4.0

The Internet of Things (IoT) and Industrie 4.0 are extremely hot topics at the moment. Instructions and commands for engines, pumps, drives, or other devices are sent sometimes via unprotected networks. The decisions about these instructions can depend on the analysis of sensor data or commands that are also sent via these networks, while remote maintenance and parameter setting also occur in public networks.

OPC UA

The protocols of the open OPC UA standards support Internet-based communication for accessing devices irrespective of their manufacturer. One typical use case is remote maintenance. The OPC-UA standard includes security specifications that are fulfilled by CodeMeter.

Authorized Components

The makers of machines and controllers have a vital interest in having only authorized components in their machines. When components or software is used from different sources, such as external suppliers or other business areas, each authorized source can be given a signature key, which is checked to verify that the software or data has not been tampered with and comes from a trusted source.

- Security-relevant tasks:
- Encrypted data (confidentiality)
- Data integrity
- Application authentication
- Access rights and user authentication
- Recording of all security incidents (auditing)
- System availability
- Licensing
- Protection against reverse engineering
- Authorized replacement parts

Advantages of the Combination Product:

- Physical dimensions
- Industrial-grade quality
- CmSecure partition for log files
- CmCdRom partition for application code
- CmPrivate partition for parameters
- CodeMeter integrated for all security functions

Conclusions

For service technicians, the combination of CmDongle and flash memory storage becomes a fully equipped, mobile test lab with maximum protection against manipulation. Mobile software for highly sensitive applications is protected ideally with a device that is easy to use and cost-efficient in administration, management, and training. Upgrading existing facilities is no problem for CmDongle with flash memory that is available in many form factors. The tiny microSD cards fit into virtually any small-scale device and are thus a feasible option for adding security to intelligent Industrie 4.0 sensors. The CmDongle with flash memory uses industrial-grade design, which provides a careful selection of components that offer high quality and remain available for long periods of time, as well as exacting tests, certification, and qualification. Manufacturers are not asking anymore whether they need to add protection technology to their products, as the added value of many devices now mostly comes from the software they are equipped with. The hardware itself is becoming more and more similar and virtually interchangeable with the standards that have been established for embedded computers and operating systems. With flexible, fine-grained licensing models, OEMs can realign their business to match this new reality. The entire software package can be optionalized with dedicated licenses to govern the right to individual functionalities. This makes life easier for product managers who now not only need to coordinate physical, but virtual differences in their product ranges as well.

Headquarters

WIBU-SYSTEMS AG
Rueppurrer Str. 52-54,
76137 Karlsruhe, Germany
Tel.: +49 721 93172-0
Fax :+49 721 93172-22
sales@wibu.com | www.wibu.com

WIBU-SYSTEMS Branch Offices

WIBU-SYSTEMS (Shanghai) Co., Ltd.
Shanghai: +86 21 556 617 90
Beijing: +86 10 829 615 60
info@wibu.com.cn

WIBU-SYSTEMS USA, Inc.
USA: +1 800 6 Go Wibu
+1 425 775 6900
sales@wibu.us

WIBU-SYSTEMS BV
The Netherlands
+31 74 750 14 95
sales@wibu-systems.nl

WIBU-SYSTEMS NV/SA
Belgium | Luxemburg
+32 3 808 03 81
sales@wibu.be

WIBU-SYSTEMS LTD
United Kingdom | Ireland
+44 20 314 747 27
sales@wibu.co.uk

WIBU-SYSTEMS IBERIA
Spain | Portugal
+ 34 91 123 07 62
sales@wibu.es

WIBU-SYSTEMS sarl
France
+33 1 86 26 61 29
sales@wibu.fr

WIBU-SYSTEMS, a privately held company founded by engineers Oliver Winzenried and Marcellus Buchheit in 1989, is an innovative technology leader in the global software license lifecycle management market.

In its mission to deliver the most secure, unique, and highly versatile technology to software publishers and intelligent device manufacturers, Wibu-Systems has developed a comprehensive, award-winning suite of hardware- and software-based solutions that incorporate internationally patented processes dedicated to protecting the integrity of digital assets, technical know-how and intellectual property.

Through its motto "Perfection in Protection, Licensing and Security", Wibu-Systems is standing up for ethically produced software and reinforces its commitment to eradicate software counterfeiting, reverse-engineering, and code tampering, while generating new digital business models fully integrated with ERP, CRM, and e-commerce platforms

SECURITY
LICENSING
PERFECTION IN PROTECTION

WIBU SYSTEMS

5062-006-02/20161118 ©2016 WIBU-SYSTEMS AG
Credits: Page 6: ©Hyperstone, Page 7 ©Hyperstone, Page 8: ©Maroxx Software GmbH, Page 9 © Wincor Nixdorf, Page 9: ©istockphoto.com/DustyPixel, Page 10: ©istockphoto.com/everlite