QONTINUUM

The physical Access Control by using memory rewritable ID tags

“fS=4”

A differential implementation

Version : U01100

Introduction

QONTINUUM

The CONACC system is a set of hardware and software, designed and built by Qontinuum, which plays a differential role in the physical Access Control where used ID tags that enable reading and writing in its memory

Contents of presentation:

- **Terminals**
- **ID tags**
- **“fS=4” structure**
- **Actors involved**
- **Current trends**
- **Resume**

Terminals

QONTINUUM

The Terminals …

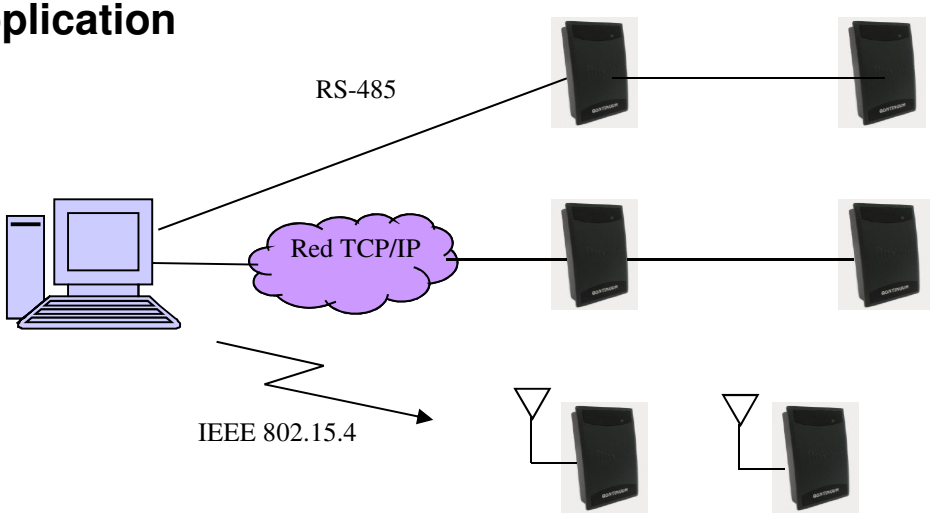
… are adaptable to various types of access points …

… by controlling one or more models of reading-writing Modules

… operating autonomously, so do not rely on communications with an application program to control the access

… can communicate with an application program through:

- ***Bus RS-485***
- ***TCP/IP (Ethernet, WiFi)***
- ***WPAN (IEEE 802.15.4)***



ID tags

QONTINUUM

The ID tags are those tangible elements that users use to get physical access to restricted areas (usually credit card shaped, but can also be a pendant or a keychain)

- **The most common are "read only" (magnetic stripe, barcode, RFID in 125 KHz or 13,56 MHz, etc.).**
- **The least common are "read-write", thus allowing the updating of information, a feature that takes advantage CONACC to establish the file system structure that we call ”fS=4” structure, which is currently applicable to ...**
  - **… contact chip-card (ISO/IEC 7816-4)**
  - **… contactless RFID tag ‘MIFARE’ (ISO/IEC 14443A-3)**
  - **… contactless RFID tag ‘DESFire’ EV1 / EV2 (ISO/IEC 14443A-4)**
  - **… “hybrid” chip-card (7816-4 + ‘MIFARE’ or ‘DESFire’)**
  - **… contactless “hybrid” RFID tag” (125 KHz + ‘DESFire’)**
  - **… NFC tags (like those on many Smart Phones)**

“fS=4” structure

QONTINUUM

We apply this name to a file system mounted on the memory of the ID tags that support reading and writing, the objective being to maximize the potential of such elements to be read but also recorded when used by holders (for instance, in "real time" during use).

For this reason, the “fS=4” structure provides more benefits than traditional systems can do by having the user information (encrypted) contained in the tags.

“fS=4” structure

QONTINUUM

The “fS=4” structure provides enough features to allow ...

… an unlimited number of users ...

... since information resides in the ID tag’s memory

... so the system use ‘Black_List' in the Terminal

“fS=4” structure

QONTINUUM

The “fS=4” structure provides enough features to allow …

… unattended data update in any Terminal prior to the access control ...

... thus enables changing the user profile identifier:

- ‘User_Group’ (affect the "when" of access)
- ‘User_Type’ (affect the “how" of access)
- ‘Pass_Levels’ (affect the "where" of access)

... and facilitates the logic administration of such ID tags:

- Unlock of anti Pass-Back control
- Reset of exhausted PIN
- etc.

“fS=4” structure

QONTINUUM

The “fS=4” structure provides enough features to allow ...

… an interactive anti Pass-Back control ...

... directly between the ID tag and the Terminal

... without need for an external program (PC) to drive it

... with control’s extinction by "temporary period exceeded"

“fS=4” structure

QONTINUUM

The “fS=4” structure provides enough features to allow ...

… biometric authentication ...

... “hand profile”

... “fingerprint” (according to standard ISO/IEC 19794-2)

... “palm vein”

... “weight” (to control the user in a floodgate)

… based on the corresponding Template contained in the “fS=4” structure

“fS=4” structure

QONTINUUM

The “fS=4” structure provides enough features to allow ...

… a truly secret PIN ...

... defined and known only by the user

... replaceable in its sole will and as often as it sees fit

“fS=4” structure

QONTINUUM

The “fS=4” structure provides enough features to allow ...

… be disabled (locked for future use) when the tag leave the installation...

... by a Terminal located in any facility’s exit point

... so it must be reactivated by any Terminal located at a facility’s entry point but always after user's biometric authentication

“fS=4” structure

QONTINUUM

The “fS=4” structure provides enough features to allow …

… different schemes of access permissions ...

... to isolate up to 16 different Operational Centers (buildings, factories, etc..) within the same Site or Installation

“fS=4” structure

QONTINUUM

The “fS=4” structure provides enough features to allow …

... full guarantee of “non cloning” ...

... in contact chip-cards:

. by the security mechanism of the ISO/IEC 7816-4 architecture

... in ‘DESFire’ tags:

. by using a Qontinuum’s algorithm that neutralizes the key breakage by "brute force“

… in App “Qtag_C” for NFC Smartphone:

. by the use of a Qontinuum mechanism that neutralizes the possible breakage of keys by "brute force" (in addition to communications encrypted by means of AES-128)

“fS=4” structure

QONTINUUM

The “fS=4” structure provides enough features to allow …

... their inclusion in a multi application’s environment t*o coexist with other applications installed before and/or later, independently and safely*

“fS=4” structure

QONTINUUM

The “fS=4” structure provides enough features to allow …

... ignore the original Serial Number of the element, whether it is the CSN (Chip Serial Number in 7816-4 and in 'MIFARE') or the UID (Unique IDentifier in 'DESFire') or the NUID (Non-Unique IDentifier in 'MIFARE'), so as to provide a complete abstraction layer in front of Serial Number duplicates.

However, 'MIFARE' should not be used because nowadays is no longer intrinsically safe.

“fS=4” structure

QONTINUUM

In summary, the “fS=4“ structure provides enough features to allow …

- **… an unlimited number of users**
- **… unattended data update in ID tag’s memory**
- **… an interactive anti Pass-Back control**
- **… many type of biometric authentication**
- **… a “secret” user’s PIN**
- **… disable the ability to use the tags upon leaving the installation**
- **… different schemes of access permissions**
- **… full guarantee that no cloning is possible for ID tags**
- **… multi applications on tags**
- **… abstraction of the original Serial Number (CSN, UID, NUID)**
- **... use Virtual accreditations (through our App "Qtag_C")**

Actors involved

Qontinuum provides the Terminals, the reading-writing Modules and the software utilities

The installation provides its own Key Administrative access to the “fS=4 structure” contained in the ID tags

The application program can be from Qontinuum (QVigila) or it can be contributed by one of our OEMs

Current trends

QONTINUUM

Since the appearance (in 1970) on the first chip-card, enough time has elapsed to make it possible to observe, in addition to a profound technological change, a change in social attitudes, so that we can now regard as a clear tendency the use of …

… contact chip-card with PKI capability (especially for logical access control, electronic signature, etc.).

... hybrid chip-card:

contact (PKI) for financial applications and/or security

+

contactless (RFID)for public transport and/or security

…Smartphone (based on NFC technology):

for "financial" and / or security applications

+
for public transport and / or security

Resume

QONTINUUM

Since 1998 we offer the CONACC system for treating ID tags endowed with “fS=4” structure, the use of which is indicated in those Installations where ...

... exist, must exist or could exist "multi applications"

... a rigorous but flexible anti 'Pass Back‘ control is needed

... must prevail the 'principle of locality' in the physical access control (independence of communications)

... security is considered a very important issue, so it is assumed as 'investment' rather than 'spending'

QONTINUUM

The physical Access Control by using memory rewritable ID tags

A Qontinuum application of great differential value