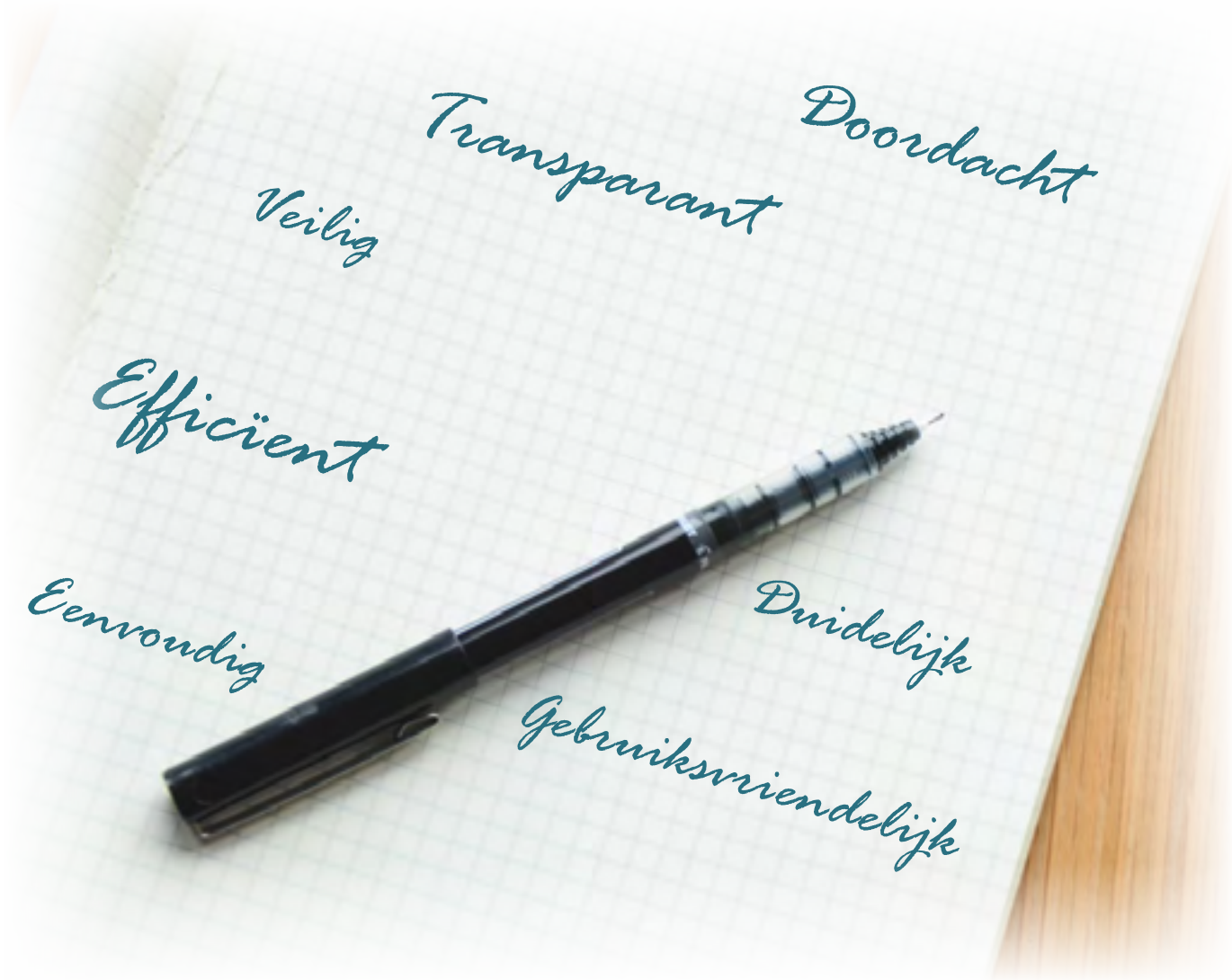
Secure Badges


Transparant
Doordacht
Veilig
Efficiënt
Eenvoudig
Duidelijk
Gebruiksvriendelijk

Secure Badges

Hoe kan je uw toegangsbadges beter beveiligen?

Dinec biedt een gebruiksvriendelijke oplossing aan voor het beveiligen van toegangsbadges.
U moet er zich vooral van bewust zijn dat om een badge te kopiëren het noodzakelijk is dat de persoon die de kopie maakt de originele badge bekomt doordat:

- ofwel de initiële gebruiker de badge aan hem geeft;
- ofwel de badge werd gestolen of slechts tijdelijk ontvreemd was.

Het is daarom van noodzakelijk belang om voor elke badgehouder ervoor te zorgen dat zijn badge niet onvrijwillig wordt gekopieerd en om het verlies van zijn badge onmiddellijk te melden. Normaal laat men zijn sleutels of creditcard ook niet rondslingeren, waarom zou men dit dan wel doen met een toegangsbadge?

In de beveiliging moet men altijd een risicoanalyse maken en de geïmplementeerde middelen verhogen om de beveiliging te vergroten. In het algemeen wordt dit aspect vaak over het hoofd gezien ten gunste van het budget.

Maar wat de badges betreft is dit financieel meer dan redelijk. Er is dus geen budgettaire reden om de beveiliging niet te verhogen.

In hoofdzaak zijn er verschillende technologieën voor badges die werken op basis van 2 frequenties:

- De 125 Khz: laat een leesafstand toe tot op maximaal 20-30 cm;
- De 13,56 Mhz: laat een leesafstand toe tot op maximaal 3-5 cm Op deze frequentie wordt tweerichtingscommunicatie geïnitieerd tussen de badge en de lezer, wat de beveiliging iets verhoogt.

In beide gevallen hebben deze badges een badge-nummer dat 'publiekelijk' toegankelijk is.
Dit wordt het CSN (Card Serial Number) of UID (Unique ID) genoemd. Dit nummer is uniek en wordt geproduceerd door de chipproducent.
Bij het hacken wordt dit nummer uitgelezen en gecodeerd op een programmeerbare kaart met gelijkwaardige technologie. Het resultaat is een hackerkaart die hetzelfde badgenummer oplevert en waarmee de fraudeur zich kan identificeren alsof hij de oorspronkelijke badgehouder is.

Dit probleem houdt op geen enkele manier verband met uw toegangscontrolesysteem. Het is gerelateerd aan de technologie van de badges.

Wij willen uw aandacht vestigen op het feit dat:

- de 125 KHz-technologie vandaag nog steeds op de markt is doordat
  1. de lezer en badges goedkoop zijn
  2. de leesafstand comfortabeler is
  3. dit nog steeds voorgeschreven wordt door de ontwerpbureaus
- Mifare-technologie wordt meer en meer toegepast, maar wordt enkel gebruikt op basis van het serienummer (CSN of UID)

De beveiliging van de badges verhogen? Hoe?

Als u zich wilt beschermen tegen illegaal kopiëren kan momenteel alleen de Mifare-Desfire-technologie met beveiligde toepassing worden gebruikt. Alle andere technologieën zijn te kopiëren of zijn gehackt op een meer of minder voor de hand liggende wijze.

Dinec toegangscontrolesystemen bieden een veilige oplossing voor uw badges

Hoe werkt het?

Twee componenten van uw toegangscontrolesysteem zijn betrokken bij deze beveiliging:

- de badge
- de lezer

Aan de badgezijde is het gebruikersidentificatienummer gecodeerd in een badgegebied dat wordt beschermd door een authenticatiesleutel en een codering op hoog niveau (AES 128 bits).

Van zijn kant ontvangt de badgelezer bij elke inschakeling de beveiligingsconfiguratie via RS-485-communicatie en heeft daarom toegang tot het gebruikersidentificatienummer en kan deze naar het toegangscontrolesysteem verzenden.

Een sleutelverhaal!

Er is één woord dat regelmatig voorkomt, en dat is het woord 'sleutel'. De codering gebeurt inderdaad op basis van beveiligingssleutels.

Je moet de badge beschouwen als een grote kast waarin je afzonderlijke vakken kunt hebben.

Er is een sleutel om de kast te openen (die de Mifare-Desfire badge voorstelt) en er is een sleutel voor elk van de afzonderlijke vakken die in de kast zijn voorzien (toepassingen die in het geheugen van de Mifare-Desfire badge zijn aangemaakt).

Met andere woorden, er is een sleutel om applicaties in de badge te maken of te verwijderen en een of meer sleutels om toegang te krijgen tot applicatie-inhoud op de kaart. Elke applicatie wordt gedefinieerd door een identificatienummer (AID).

Het volgende moet gedefinieerd worden:

- Een aanvraagnummer (AID).
- Een toegangssleutel voor deze applicatie.
- Een sleutel die de kaart beschermt (optioneel).

Het principe is dat de lezer geprogrammeerd is om uitsluitend de inhoud van een beveiligde toepassing te lezen.

Secure Badges

Dinec heeft gekozen voor openheid en gebruiksvriendelijkheid.

Sommige leveranciers bieden mogelijk beveiligde kaarten aan, maar heel vaak blijven ze eigenaar van uw beveiliging.

In feite bieden ze lezers en kaarten aan waarbij alleen zij de beveiligingssleutel of de programmering van de lezers bezitten.

Dit bindt de klant aan de leverancier en dwingt de klant om de kaarten te kopen van één enkele leverancier die dus de prijszetting kan doen zoals hij wenst.

Dinec heeft ervoor gekozen om de klant de mogelijkheid te bieden zijn eigen beveiligingssleutel te definiëren en zijn kaarten te formatteren via een speciaal ontwikkelde encoder om de kaart te beveiligen.

Concreet

- U moet een uniek identificatienummer coderen in een Mifare-Desfire-badge en meer in het bijzonder in een applicatie die wordt beschermd door een sleutel.
- DA-5003 / DA-5013-lezers moeten zo worden geconfigureerd dat ze de inhoud van deze beschermde toepassing kunnen lezen.

Vanuit materiaal oogpunt moet u het volgende hebben:

- Een Dinec-systeem met een geüpdatet softwareversie met beveiliging (DA400/DBM6000)
- Dinec DA-5003/DA-5013 lezers
- Mifare - Desfire-kaarten (DA-1897/DA-1877/DA-1899)
- De Androïd-toepassing voor DMB6000 (voor Smartphone met NFC-optie)

Vanuit het standpunt van het systeem

In het configuratiemenu van de lezers worden het gebruikersnummernummer en de beveiligingssleutel gedefinieerd. Merk op dat de toegangscode voor de kaartconfiguratie vrij is gelaten. Hierdoor kan de klant immers andere toepassingen aan de kaart toevoegen om deze ook voor andere oplossingen te gebruiken (fotokopieermachine, e-wallet, enz.). Uiteraard maakt dit het formatteren van de kaart ook mogelijk, maar formatteren leidt niet tot een beveiligingslek. De kaart wordt verwijderd en wordt niet meer geaccepteerd.

Nadat deze parameters zijn ingevoerd, worden de DA-5003 / DA-5013-lezers automatisch geconfigureerd om dit beveiligde gebied te kunnen lezen. Op dezelfde manier zal de Androïd applicatie deze parameters ontvangen om deze beveiligde zone te kunnen creëren in de Mifare-Desfire badge.

Vanuit het standpunt van de lezer

Er hoeft geen actie te worden ondernomen met de lezer. De beveiligingsconfiguratie wordt automatisch naar de lezer gestuurd. Als een lezer wordt losgekoppeld of uitgeschakeld, verliest deze automatisch zijn sleutel. De beveiliging wordt opnieuw geprogrammeerd zodra de lezer terug aangesloten wordt op de installatie.

Vanuit het standpunt van de Smarthpone toepassing

De beveiligde instellingen worden naar de applicatie overgedragen via WiFi of door bestanden over te brengen naar de applicatiemap. Bij het beheer van de badges van de applicatie kan door het kiezen van de Secure-optie de badge worden geformatteerd en kan de applicatie worden aangemaakt met zijn identificator.

Als uniek identificatienummer hebben we ervoor gekozen om ofwel het serienummer van de badge (CSN-UID) ofwel ditzelfde nummer vooraf te laten gaan door het voorvoegsel 1 te coderen.

De keuze van het serienummer heeft de volgende voordelen:

- Het is niet nodig om de badges te hercoderen in het geval van een bestaande installatie waarbij het serienummer wordt gelezen. De klant kan zijn badges opmaken en overschakelen naar de beveiligde modus wanneer alles klaar is.
- LCT-5006-operatorlezers kunnen zonder enige herconfiguratie worden gebruikt.
- Een garantie voor het unieke karakter van het badgenummer zonder risico op duplicatie.

Secure Badges

Nog meer beveiliging !!

Diversificatie van sleutels

Er bestaat een optie om de sleutels te diversifiëren. Dit verhoogt de beveiliging.

Inderdaad, laten we ons voorstellen dat iemand erin slaagt om de veiligheidssleutel te leren kennen. En dit ondanks het feit dat het iets is dat verborgen en geheim moet blijven.

Hij zou elke badge op het systeem kunnen namaken, omdat hij de sleutel kent.
De lezer zou de inhoud van de applicatie lezen en een correct nummer vinden.
Wanneer diversificatie wordt geactiveerd, is de toegangssleutel tot de applicatie verschillend voor elk van de badges. Deze sleutel is het resultaat van een complex algoritme waarmee rekening wordt gehouden met:

- het serienummer van de kaart (CSN-UID)
- de beveiligingssleutel
- een Dinec-specifieke sleutel

Een kaart die niet is geformatteerd door de Dinec-applicatie kan daarom niet worden gelezen!

Een verhaal sinds 1981

In de hoedanigheid van baanbreker, ontwerper en fabrikant sinds 1981, ontwikkelt en verhandelt Dinec International tevens beveiligingssystemen, tijdbeheersoplossingen en gebouwbewakingsoplossingen. Onze teams stellen zich tot doel systemen te ontwikkelen die zijn uitgerust met moderne en efficiënte technologieën. Met onze systemen handhaven we de integriteit van uw onroerend of industrieel erfgoed en vergemakkelijken we tegelijkertijd het dagelijks technisch en administratief beheer ervan.

Dankzij de nabijheid van ons ontwikkelingskantoor en onze productie-eenheid in België, verzekeren we ons van een perfecte symbiose met het oog op de controle en kwaliteit van onze systemen.

Ons assortiment

- Toegangscontrole met badges, vingerafdrukken of een toetsenbord
- Beheer van bezoekers
- Anti-inbraakalarm
- Technische bewaking van gebouwen
- Statistisch toezicht
- Beheer van parkeerruimte
- Video bewaking
- Beheer van aanwezigheden
- Energiebeheer
- Toezicht op rondes

DINEC INTERNATIONAL
BELGIUM

Chaussée de Louvain 592
B-1380 Ohain

+32 (0)2 389 16 40
+32 (0)2 387 14 02
contact@dinec.be
www.dinec.be

PUBP0283-13/03/2020