

# INFO-ARK: ID-KORT

- » Sikkerhed og valgfrihed
- » Læseafstande
- » Fordele og ulemper
- » Kombinerede løsninger

## BERØRINGSFRIE KORTTEKNOLOGIER

Alle adgangskontrolsystemer bruger en form for kortteknologi - ofte er det et magnetkort eller en adgangsbrik, andre gange et adgangskort, og i andre tilfælde en langtrækkende brik til bilen. I dette her info-ark vil vi forklare baggrunden for nogle af de berøringsfrie teknologier der findes, og dermed være med til at skabe større klarhed over hvilke muligheder og begrænsninger der eksisterer.

## FUNKTION

De berøringsfrie adgangskort eller adgangsbrikker har alle en chip indbygget, som, når den præsenteres for kortlæseren, afgiver et ID til denne. Der findes mange forskellige måder at håndtere denne kommunikation på, og hver måde har sine fordele og ulemper.

## LÆSEAFSTAND

Læseafstanden er ofte det som de fleste kunder interesserer sig for. Man vil måske gerne have sit adgangskort læst uden at skulle have det op af lommen, eller man stille krav om automatisk læsning—det der kaldes håndfri læsning. I mange tilfælde vil disse ting kunne lade sig gøre, dog kræver det at man stiller de rigtige krav til teknologien - med lidt god planlægning og test af de enkelte produkter, vil man kunne lave den helt rigtige kombination af læseafstand og sikkerhed.

## TEKNOLOGI OG FORMATER

Den teknologi som chippen anvender til at sende sit ID nummer på, kaldes ofte for ID-teknologien. Det kan være EM (EM4001, EM4102 etc.), MIFARE (UltraLight, Classic, DESFire, Plus), HID iCLASS, HID Prox, Legic eller Nedap NeXS. Disse teknologier anvender forskellige frekvenser (typisk 125 KHz eller 13,56 MHz) og nogle har også mulighed for at opbevare data i chippen (MiFARE og iCLASS).

Selve ID-nummeret dannes af et binært tal der er lagret i chippen. Dette tal er lagret i et bestemt format, som kan være af forskellige størrelse/længde - typisk taler man om 26 bit format, som betyder at ID-nummeret består af ialt 26 bit. Formatet bestemmer hvordan det binære tal skal tolkes af adgangskontrolsystemet, og dermed hvordan de 26 bit bliver til et tal der er "forståeligt".



## FACTS

### → Sandheden om formater

Formatet inde i adgangskortet kan være åbent eller lukket (administreret, slutkunde-ejet eller leverandør-ejet). Dette siger noget om hvilken binding man har til en given leverandør.

De **åbne formater** er offentligt tilgængelige - dvs. alle kan bruge dette format. Det svarer til at man har en offentlig tilgængelig standard for udveksling af data, og derfor er man i princippet meget frit stillet i forhold til hvor man vil købe sine adgangskort. Da formatet er offentligt tilgængeligt, er der en teoretisk risiko for at opleve dubletter da alle kan købe nye kort med det åbne format.

De lukkede formater består af primært 3 typer:

**Administreret format** - kortformatet administreres af en leverandør, og her er det leverandøren der garanterer at man ikke oplever dubletter. Leverandøren registrerer hvilke kort der er produceret til hvilken kunde, hvorved der ikke kan ske dublet leverancer.

**Slutkunde-ejet format** - her er det slutkunden som ejer formatet - dvs. slutkunden kan vælge hvor adgangskort skal købes. Dette betyder at man som slutkunde er frit stillet i forhold til leverandører, samtidig med at man teoretisk set ikke kan opleve dubletter.

**Leverandør-ejet format** - her er det leverandøren (typisk producenten af systemet eller forhandleren) der ejer formatet. Dette betyder at man er bundet til denne, og meget ofte er det umuligt at komme ud af den binding. Formatet er typisk helt lukket, og det ses også at adgangskortet og kortlæserne er låst til hinanden, hvorved man bliver nødt til at udskifte både kortlæser og adgangskort for at skifte leverandør.

### → De "frække" spørgsmål:

Stil følgende spørgsmål til din leverandør af ID-kortteknologier:

1. Hvem "ejer" mit format - er det leverandøren/installatøren, producenten, og kan jeg selv overtage ejerskabet?
2. Hvordan bliver jeg stillet frit - og hvad er omkostningerne forbundet med det?
3. Kan jeg få et kombineret kort, der både giver mig lang læseafstand og mulighed for at gemme data på kortet?
4. Kan jeg opgradere sikkerhedsniveauet på mine kort på et senere tidspunkt?
5. Hvilken binding til installatør/leverandør har mine kortlæsere? Bruger de åbne formater?

# MIFARE-TEKNOLOGIEN

## HVAD ER MIFARE?

MiFARE standarden stammer fra ca. 1994 og blev oprindeligt defineret af Philips. Den blev opfundet til elektronisk billettering, og blev senere udbredt som en slags de-facto standard indenfor sikringsbranchen.

Læseafstanden er typisk mellem 2-6 cm, og sjældent mere end 8 cm. Læseafstanden bestemmes hhv. af størrelsen på læseren og spolen i adgangskortet, og jo større spole i adgangskortet, jo længere læseafstand. Den er defineret i en ISO standard 14443A og dette er basis for den åbne platform som MiFARE kendetegnes ved.

Nogle af argumenter for MiFARE kortet er selve multi-funktionaliteten, som betyder at man på eet og samme kort kan lægge flere funktioner. Da man har en åben standard samtidig med at man kan skrive til kortet, giver dette mulighed for at flere leverandører kan tilgå informationerne på kortet. Dette benyttes til adgangskontrol, kantinebetaling, printeradgang (print-on-demand),

## UDGAVER

MiFARE teknologien findes i flere udgaver. De mest udbredte i Danmark er S50 1K og S70 4K - som beskriver hvilken chip der er benyttet og hvor meget hukommelse der er i chippen. Der findes også version kaldet Ultira Light, DUAL og DESFire. DESFire er relativt udbredt i USA, hvilket skyldes en bedre krypteringsmetode og større og mere fleksibel hukommelse.

## MIFARE KONTRA ICLASS

MIFARE kan sidestilles rent opbygningsmæssigt med iCLASS. Dog er der en sikkerhedsmæssig forskel på MiFARE og iCLASS til fordel for iCLASS. iCLASS bygger også på en ISO standard (ISO15693), og der er flere og flere producenter der understøtter standarden bag iCLASS chippen.

iCLASS funktionaliteten er opfundet af HID, og nogle af de primære fordele fremfor MiFARE er læseafstanden og muligheden for at få adgangskort og kortlæsere der på forhånd er konfigureret med det format, som man er sikker på ikke eksisterer andre steder i verden.

Så længe man vælger HID's krypteringsnøgler er man afhængig af HID (da de koder kortene og kortlæserne), men man kan vælge at få sin egen nøgle, hvorefter man kan købe sine adgangskort andre steder. HID iCLASS læserne er billigere end de fleste tilsvarende MiFARE-læsere, og samtidig er der livstidsgaranti på HID iCLASS læsere.

## MIFARE DESFIRE

MIFARE DESFire er den MiFARE standard der sikkerhedsmæssigt er sammenlignelig med HID iCLASS. Den er relativt ny i Skandinavien, og derfor ikke særlig udbredt. MIFARE DESFire har nogle af de samme krypteringsteknologier som iCLASS og er også en åben standard/platform.

## MIFARE LÆSERE

→ **HID iCLASS og MultiCLASS** læsere kan alle læse MiFARE CSN og kan levere det i flere formater (26, 32, 34, 40 bit). MiFARE DESFire CSN kan læses efter en omkonfiguration, og giver et højere output (56, 64 bit) som de færreste adgangskontrolsystemer kan forstå. Der er mulighed for et kortere format, men dette giver teoretisk mulighed for dubletter i systemet. Formatoutputtet konfigureres enten fra fabrikken eller på læseren vha. et konfigurationskort.

→ **HID iCLASS og MultiCLASS** læsere kan alle læse MiFARE CSN og kan levere det i flere formater (26, 32, 34, 40 bit). Formatoutputtet konfigureres enten fra fabrikken eller på læseren vha. et konfigurationskort.

→ **IDESCO Access 7C** læser også MIFARE CSN og kan outputte som standard i enten 26 eller 32 bit.

→ **IDESCO Access 8CM** læser **sektorerne** på MiFARE kortet, og kan sættes op vha. konfigurationskort. Krypteringsnøgler lagres i kortlæseren.

→ **HID/Vitani SmartID** læser **sektorerne** på MiFARE kortet, og kan sættes op vha. konfigurationskort. De fås også i en udgave som kan læse DESFire Folders (som svarer til MiFARE Sektorer). SmartID kan leveres i en DUAL MiFARE læser der kan læse 2 separate MiFARE opsætninger.

→ **Nedap Inveox** læser enten fra **sektorerne** eller **CSN** nummeret. Konfigurationen af læseren kan ske med konfigurationskort eller fra Nedap softwaren - dvs. man kan centralt ændre i opsætningen af hvordan læseren skal håndtere krypteringsnøgler etc. Nedap Inveox læser også DESFire

# MIFARE CSN KONTRA SEKTORLÆSNING

## CSN

CSN (Card Serial Number), også kaldet UID (Unique Identifier), er det 32 bit nummer som enhver MiFARE-chip indeholder. Den defineres på fabrikken, og er i teorien unik. MiFARE DESFire har et 64 bit CSN/UID.

Mange læsere læser dette nummer, og sender det over wiegand til adgangskontrolsystemet. Mange systemer kan læse disse data direkte, mens andre systemer afkoder data og "forkorter" data. Dette kan give en teoretisk risiko for dubletter.

Nogle læsere kan leveres med 26 bit MiFARE eller DESFire CSN output, og dette betyder at det er læseren der forkorter data. Et IDESCO 26 bit CSN output fjerner de mindst betydende bits, mens et HID 26 bit CSN output udover at fjerne data, også lægger en facilitykode ind og i princippet får man et 26 bit HID format ud af CSN nummeret. Der er stadig risiko for dubletter når der ikke anvendes samtlige 32 bit hhv. 64 bit. Nedap AEOS har mulighed for at læse alle 64 bit.

Fordelen ved at bruge CSN er, at man kan læse alle typer MiFARE brikker og man derfor ikke binder sig til at købe adgangskort fra een bestemt leverandør. Bruger man de 32 eller 64 bit er der ingen risiko for dubletter, og det kan da anbefales at bruge en USB Bordlæser til at indlæse kortene med (da numrene er meget kryptiske).

CSN er sikkerhedsmæssigt på niveau med traditionelle proximity (EM, AWID) teknologier. Sikkerhedsmæssigt er CSN ikke på niveau med en HID Proximity (med lukkede formater), da der ingen central kontrol er med hvilke chip's der har hvilke numre.

## SEKTOR/FOLDER DATA

I selve MiFARE chippen er der nogle sektorer, som kan sammenlignes med "foldere" på en harddisk. Disse sektorer kan indeholde data, og dem kan man bruge til at lægge adgangskort-numre ned i. Dette betyder at man selv kan vælge hvilket format data skal lægges ned i, og man har mulighed for at beskytte disse data med nogle krypteringsnøgler som man evt. selv kan definere. Hvis man selv har defineret nøglen, har man stadig mulighed for at købe MiFARE kort hvor som helst, men til gengæld skal man have udstyr som kan skrive ned på MiFARE kortet. Dette kan ske fra en kortprinter eller en MiFARE kort-koder. Nogle MiFARE læsere kan også skrive til kortet.

På samme vis som man lægger adgangskort-numre ned på en sektor, kan man også lægge en eller flere fingeraftryksskabeloner ind på MiFARE kortet.

De MiFARE læsere der bruges til at læse sektorerne med, er ofte en lille smule dyrere end de læsere der blot læser CSN nummeret. Dette skyldes brugen af en mere avanceret MiFARE læserchip.

I MiFARE DESFire benævnes sektordata som foldere.



IDESCO Access



HID RK40 iCLASS/MIFARE



Nedap Invexs MIFARE DEFIRE med display

# SAMMENLIGNINGSKEMA

- » Sikkerhed og valgmuligheder
- » Læseafstande
- » Fordele og ulemper
- » Leverandørbinding

Teknologi	Format	Sikkerhed	Leverandørbinding	Læseafstand	Fordele	Ulemper
MiFARE CSN	Åbent (26 bit)	I praksis ses dubletter.	Ingen	2-8 cm	Kræver ingen programmering af adgangskort	Numre er typisk 32 bit og aldrig fortløbende, risiko for dubletter, mange ældre systemer kan ikke udnytte hele nummeret og må "skære" tal af, med større risiko for dubletter <b>Producenten anbefaler ikke denne teknologi til nye løsninger</b>
MiFARE CSN	Åbent (32 bit)	Teoretisk er der ikke dubletter	Ingen	2-8 cm	Kræver ingen programmering af adgangskort	Numre er typisk 32 bit og aldrig fortløbende, mange ældre systemer kan ikke udnytte hele nummeret og må "skære" tal af, med risiko for dubletter <b>Producenten anbefaler ikke denne teknologi til nye løsninger</b>
MiFARE Sektorkodning	Typisk lukkede	Relativt god sikkerhed, mulighed for selv at bestemme nummerserien, teoretisk kloningsrisiko	Ofte, ikke altid muligt at ophæve bindingen	2-8 cm	Mulighed for at bestemme egen nummerserie	Kræver kodning af kort, kræver specielle (dyrere) læsere som oftest er låst af leverandøren. Ofte er man bundet til leverandøren af adgangskortene, læserne eller adgangskontrolsystemet <b>Producenten anbefaler ikke denne teknologi til nye løsninger</b>
MiFARE DESfire CSN	Åbent	Teoretisk er der ikke dubletter	Ingen	2-8 cm	Kræver ingen programmering af adgangskort	Numre er typisk 64 bit og aldrig fortløbende, mange ældre systemer kan ikke udnytte hele nummeret og må "skære" tal af, med større risiko for dubletter
MiFARE DESFire Folder	Åbent eller lukket	Høj sikkerhed, høj krypteringsniveau, mulighed for selv at bestemme nummerserien	Ofte, ikke altid muligt at ophæve bindingen	2-8 cm	Høj sikkerhed, mulighed for at bestemme egen nummerserie	Kræver kodning af kort, kræver specielle (dyrere) læsere som oftest er låst af leverandøren. Ofte er man bundet til leverandøren af adgangskortene, læserne eller adgangskontrolsystemet
Nedap NeXS	Lukket	Meget høj sikkerhed, ingen risiko for dubletter	Man er bundet til producenten af systemet, men ikke leverandøren/installatøren	2-95 cm	God læseafstand (berøringsfri og håndfri aflæsning), sammenhængende nummerserie	Man er bundet til selve producenten (på samme vis som man ofte i forvejen er bundet til producenten rent software- og hardwaremæssigt)
iCLASS 26-bit HID	Åbent	Teoretisk risiko for dubletter	Ingen	2-40 cm	Sammenhængende nummerserie	Teoretisk risiko for dubletter da det er et helt åbent format.
iCLASS Vitani format	Lukket	Ingen risiko for dubletter	Kan ophæves	2-40 cm	Sammenhængende nummerserie, mulighed for at bestemme nummerserie selv	Formatet kan kun købes hos Vitani, men det er muligt at bruge adgangskort fra andre leverandører samtidig med Vitani adgangskort - dvs. ingen bindinger
iCLASS Elite (krypteret)	Åbent eller lukket	Høj sikkerhed, høj krypteringsniveau, mulighed for selv at bestemme nummerserien	Kan ophæves	2-40 cm	Høj sikkerhed, mulighed for at bestemme egen nummerserie	Formatet kræver ekstra administration i forhold til alle øvrige formater

# FAQ: MIFARE SIKKERHED

- » TYPISKE SPØRGSMÅL OMKRING MIFARE SIKKERHED
- » PRODUCENTENS FAQ
- » [HTTP://WWW.NXP.COM/CGI-BIN/FAQ/FAQ.PL?QUERY=G&ID=41&FID=18](http://www.nxp.com/cgi-bin/faq/faq.pl?query=g&id=41&fid=18)

## PRODUCENTENS FAQ

### Q: What is exactly the discussion around MIFARE Classic?

A: NXP has come to the conclusion that up to date 3 research groups have retrieved the algorithm and developed attacks to break keys of MIFARE Classic-enabled cards within seconds. These are the group around Karsten Nohl, who initially presented the reverse engineering of MIFARE Classic chips in December 2007 at the 24th Chaos Computer Congress in Berlin, the IT security specialists from the Radboud University of Nijmegen as well as Nicolas T. Courtois from the University College London. The Nijmegen University intends to present a publication during a conference on October 6th, with information on how the protocol and algorithm were reverse engineered, the description of the protocol and algorithm and the description of some practical attacks which can be carried out with limited means.

### Q: What does this mean for my system? Is it possible that the cards of my system can be cloned?

A: Whether or not a card can be cloned depends on how the system is designed. There are countermeasures possible which limit the risk, but it cannot be fully excluded. However NXP expects that in many systems no or little of such countermeasures are actually implemented.

### Q: How is NXP going to prevent the publication of the algorithm?

A: We have clearly explained to the research groups the potential risks that such a publication would entail and tried to delay the publication planned by the University of Nijmegen with an injunction. However the court in Arnhem decided per July 18th to allow the publication. This report will reduce the barrier to carry-out actual attacks on infrastructures using MIFARE Classic, which prompted our request for a delay in its publication in order to allow for reasonable time for appropriate system security upgrades. The NXP technologies are protected by many intellectual property rights of different nature. Should it appear that any NXP rights (in the broadest sense of the word) have been illegally compromised, NXP will immediately take the appropriate action.

### Q: Which products of the MIFARE family are referred to?

A: The attacks exclusively refer to NXP's MIFARE Classic chips comprising the MIFARE Mini, MIFARE 1k and the MIFARE 4k as well as its emulations. The attacks do not refer to other MIFARE products like MIFARE DESFire or MIFARE Plus.

### Q: When did NXP know of the MIFARE Classic attack and what did you do about it?

A: We learned of the hack on the 31st December 2007 and immediately assembled a task force to deal with the issue. We have been assessing various implications of the vulnerabilities and been in contact with system integrators since then. NXP is also in direct contact with the research groups and has evaluated their attacks. Although not all vulnerabilities in MIFARE Classic-based infrastructures can be fixed short-term, we identified countermeasures to make the attacks more difficult in order to strengthen the end-to-end security of existing designs, shared these with our partners and continue to do so.

### Q: I am using MIFARE Classic in my infrastructure. What shall I do to prevent any security issues?

A: Please contact your system integrator as soon as possible to assess whether your systems would need any additional security measures in the light of the above.

### Q: What do you recommend for existing installations using MIFARE Classic?

A: In general NXP recommends extensive additional protection mechanisms in MIFARE Classic infrastructures, both on how the data on the card is used as well as deploying additional security layers separate from the card. The system integrators who have designed MIFARE Classic-based installations should review them in light of the existing vulnerabilities, in light of the value of the assets that are protected and in relation to other means of protection and fraud detection in place. Thus they can judge if these systems can remain as they are, if they would require additional measures or if a security upgrade is needed.

### Q: Can NXP fix the compromised infrastructures?

A: NXP's expertise is the design and manufacturing of chips; although we do not design end to end security systems, we would be happy to continuously support your system integrator so that the best solutions are reached.

### Q: What does that mean exactly for access management systems?

A: End to end measures should also be applied for access management infrastructures, which are typically complemented by additional measures e.g. camera surveillance, security personnel, etc. when valuable assets need to be protected. We recommend that the assessment of the impact of the recent and expected developments takes into account the particular way that the system is implemented and used, its relation to other protection in place, and specifically whether there is a need to prevent unauthorized single time access or access during a limited period of time. Depending on the specific situation in existing MIFARE Classic access management infrastructures the usage of more sophisticated card ICs may be an alternative to implementing sufficient countermeasures. **DESFire EV1 and MIFARE Plus are our recommended solution for new access management implementations where a strong level of security is required to protect against a one time unauthorized access.**

### Q: What will NXP do to prevent attacks from hackers?

A: Attacks targeting IC security are part of the normal lifecycle of security products, like viruses on computers. NXP is continuously improving the security level of existing product ranges as well as creating new product ranges with best in class security, e.g. the new DESFire EV1 chip or our recently announced a new member of the MIFARE family, the MIFARE Plus. Both, MIFARE Plus and our high-end product MIFARE DESFire EV1 offer strong AES encryption and are targeted to receive the internationally recognized 3rd party Common Criteria security certification.