Toekomstvaste fysieke toeg

Zonder beveiliging is een elektronische toegangpas makkelijk na te maken. Als niemand meer aanwezig is, heeft een indringer met zo'n nagemaakte pas vrij spel. Om dit tegen te gaan wordt cryptografie toegepast voor beveiliging van de communicatie tussen pas en lezer. Vrijwel altijd is dit symmetrische cryptografie. Asymmetrische cryptografie is beter, maar was tot voor kort op contactloze systemen praktisch niet te gebruiken. Inmiddels kunnen nieuwe systemen echter gebruik maken van asymmetrische cryptografie en aansluiten bij bestaande systemen voor toegang tot ICT die al gebruik maken van asymmetrische cryptografie.

Voor de fysieke toegangsregulering tot ruimten en gebouwen maken veel organisaties gebruik van elektronische toegangsystemen. Iemand die toegang wil, dient zich eerst te identificeren. Op basis van aan de identificatie gekoppelde autorisaties bepaalt het systeem dan of de betreffende persoon toegang wordt verleend. De identificatie vindt veelal plaats door het aanbieden van een elektronische pas of tag. Deze heeft meestal een contactloze chip met identificatie-informatie. Vaak staan op de pas ook een foto en persoonsgegevens voor visuele controle. Ook worden passen uitgerust met een contactchip voor toegang tot ICT en/of het plaatsen van een digitale handtekening (*1). Zo'n contactchip wordt doorgaans beveiligd volgens het principe van de Public Key Infrastructure (PKI).

Management-summary

Voor fysieke toegangsystemen wordt veelal gebruik gemaakt van toegangpassen met een contactloze chip. Soms zijn deze passen ook nog voorzien van een PKI (Public Key Infrastructure) contactchip voor toegang tot ICT en/of het plaatsen van een digitale handtekening. Ook voor fysieke toegangsystemen biedt PKI een groot aantal voordelen. Organisaties die aanschaf of vervanging van toegangspassen overwegen, kunnen de fysieke toegang beter op basis van PKI inrichten. In de VS is dit inmiddels een trend aan het worden.

Authenticatie Een contactchip is ook voor fysieke toegangsystemen te gebruiken, maar de voorkeur gaat uit naar een contactloos principe. Dat werkt gebruikersvriendelijker en is minder gevoelig voor slijtage. Hoe het uitwisselen van informatie precies verloopt, verschilt per merk. Wel wordt bij professionele systemen in de regel gebruik gemaakt van encryptie om misbruik van de communicatiesignalen tegen te gaan. Het gaat dan in de regel om symmetrische cryptografie. Zowel de chip op de pas als de lezer beschikken over een geheime sleutel. Zodra de pas vlakbij de lezer komt, controleren beide bij elkaar de aanwezigheid van de juiste sleutel. Deze wederzijdse authenticatie zorgt ervoor dat de pas zijn identificatiecode pas vrijgeeft als hij weet dat de paslezer te vertrouwen is. De paslezer kan er op zijn beurt op vertrouwen dat de aangeboden pas 'echt' is. Het authenticatieprotocol beveiligt tegen het eventuele afluisteren, manipuleren of opnieuw uitzenden van het signaal door een indringer.
De geheime sleutel die gebruikt wordt door een toegangsysteem binnen één individueel bedrijf is vaak gelijk voor alle passen en paslezers. Door het authenticatieprotocol kan een sessiesleutel worden afgesproken waarmee de communicatie tussen de pas en de paslezer wordt beveiligd tegen afluisteren. De contactloze chip wordt beschouwd als een veilig opslagmedium. Deze chip is zodanig ontworpen dat de sleutel moeilijk kan worden achterhaald. En zonder sleutel is de informatie op de kaart niet te ontcijferen.

PKI Historisch gezien is het begrijpelijk dat bij fysieke toegangsystemen gebruik wordt gemaakt van contactloze chips met symmetrische cryptografie. Inmiddels is het echter technisch mogelijk om asymmetrische cryptografie te gebruiken in combinatie met een contactloze interface. Net zoals PKI wordt gebruikt voor toegang tot ICT, kan deze vorm van asymmetrische cryptografie worden gebruikt in contactloze systemen voor fysieke toegangverlening. In Europa ziet het er nog niet naar uit dat leveranciers van fysieke toegangsystemen asymmetrische cryptografie en PKI op korte termijn gaan ondersteunen. In de Verenigde Staten is er wel een sterke trend om PKI te gebruiken (*2). Dat wordt mede ingegeven door de federale overheid die het gebruik van PKI voor fysieke toegang sterk aanbeveelt (zie FIPS 201-1 (*3), NIST SP 800-116 (*4) en FIPS 201-2 Draft (*5)) en mogelijk in de toekomst zelfs verplicht zal stellen.

Standaardisatie Sommige organisaties gebruiken zowel een contactloze chip als een contactchip met PKI op één pas. In zo'n geval zou ook voor één chip met PKI voor zowel toegang tot gebouwen als ICT gekozen kunnen worden. Deze is contactloos uit te voeren, zodat ook voor ICT-toegang de gebruikersvriendelijkheid toeneemt. Bovendien worden voor de organisatie het sleutelbeheer en het pasbeheer vergemakke-

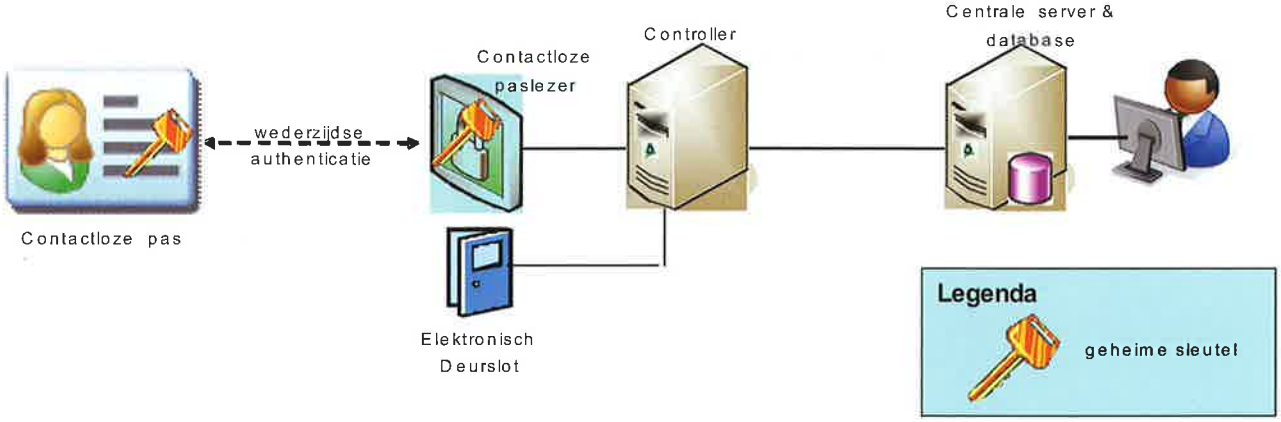
angsystemen

lijkt, omdat nog maar één chip per pas gepersonaliseerd hoeft te worden.
In tegenstelling tot fysieke toegangsystemen waar de systemen gesloten zijn en er geen standaardisatie is wat betreft het gebruik van cryptografie en informatie op één pas, zijn er voor PKI en smartcards veel open standaarden. Deze leggen aspecten vast zoals certificaatprofielen (X509), controle op geldigheid (OCSP, CRL) en gebruik van cryptografie op een smartcard (ISO/IEC 7816-15:2004) (*6). PKI is een volwassen techniek die op grote schaal overal ter wereld wordt toegepast. Door de standaardisatie is er een hoge mate van interoperabiliteit tussen componenten van verschillende leveranciers, zoals paslezers en PKI-chips. Zo is gebruik van PKI op een smartcard ook onafhankelijk van het gebruikte PKI-chipplatform. Daardoor kan vrij eenvoudig worden overgestapt op een ander platform en/of leverancier. De standaardisatie maakt ook een verandering in lengte van sleutels en/of gebruik van een ander cryptografisch algoritme relatief eenvoudig.

Kwetsbaar Wat betreft functionaliteit is het sleutelbeheer bij fysieke toegangsystemen veelal erg beperkt. Er wordt meestal één geheime sleutel gebruikt die aanwezig is in alle passen en paslezers. Dit gaat ten koste van de flexibiliteit en maakt het systeem bovendien kwetsbaar. Het compromitteren van de enige geheime sleutel maakt het gehele toegangsysteem onbetrouwbaar. Daarbij is het de fabrikant of leverancier die de sleutel vaststelt en niet de gebruiker van het systeem. Het periodiek veranderen van de sleutel is dan ook doorgaans niet mogelijk.
Voor gebruik van PKI is sleutelbeheer daarentegen noodzakelijk. Dit wordt anders ingericht dan het sleutelbeheer voor symmetrische sleutels. Het voornaamste verschil betreft de paslezers waarvoor het sleutelbeheer eenvoudiger is. Deze hoeven namelijk niet meer te worden voorzien van een geheime sleutel via in-line sleuteldistributie of zogenaamde masterkaarten, maar controleren op basis van een publieke sleutel de digitale handtekening en de geldigheid van het certificaat.

Vertrouwen Door gebruik van PKI zijn de paslezers minder kwetsbaar voor het lekken van sleutels. Er is immers geen geheime sleutel die beschermd hoeft te worden. Alleen op de passen zijn de privésleutels opgeslagen die geheim dienen te blijven. De kwetsbaarheid van de passen verschilt hier echter niet wezenlijk met fysieke toegangsystemen zonder PKI. Wijzigingen om de kwetsbaarheid te verhelpen kunnen gefaseerd worden doorgevoerd door uitrol van nieuwe passen. Dat is minder complex dan het aanbrengen van wijzigingen aan alle paslezers.
Gebruik van PKI binnen fysieke toegangsystemen biedt de organisatie ook flexibiliteit om toegang te verlenen op basis van identificatiemiddelen die zijn uitgegeven door andere organisaties. De paslezers hoeven immers geen geheime sleutel te kennen om de echtheid van een pas en de informatie op de pas te kunnen controleren. Wat geregeld moet worden is dat men vertrouwen heeft in de andere organisatie en dat binnen fysieke toegangsystemen autorisaties kunnen worden verleend op basis van een identiteitskenmerk van een andere organisatie.

Conclusies Het gebruik van PKI voor fysieke toegang betekent een andere inrichting van sleutelbeheer die een betere beheersing van het risico voor toegangbeheer mogelijk maakt. Aangesloten kan worden bij een reeds bestaande PKI voor toegang tot ICT. Paslezers worden minder kwetsbaar doordat er geen geheime sleutels in opgeslagen zijn. Ze moeten echter wel gekoppeld worden met een netwerk om de status van certificaten te kunnen controleren. PKI geeft ook de flexibiliteit om gefaseerd over te stappen op andere technologie en leveranciers. Deze synergie geeft zowel kostentechnische voordelen, maar ook beveiligingstechnische wanneer bepaalde componenten kwetsbaar blijken te zijn, zoals een chip- ▸

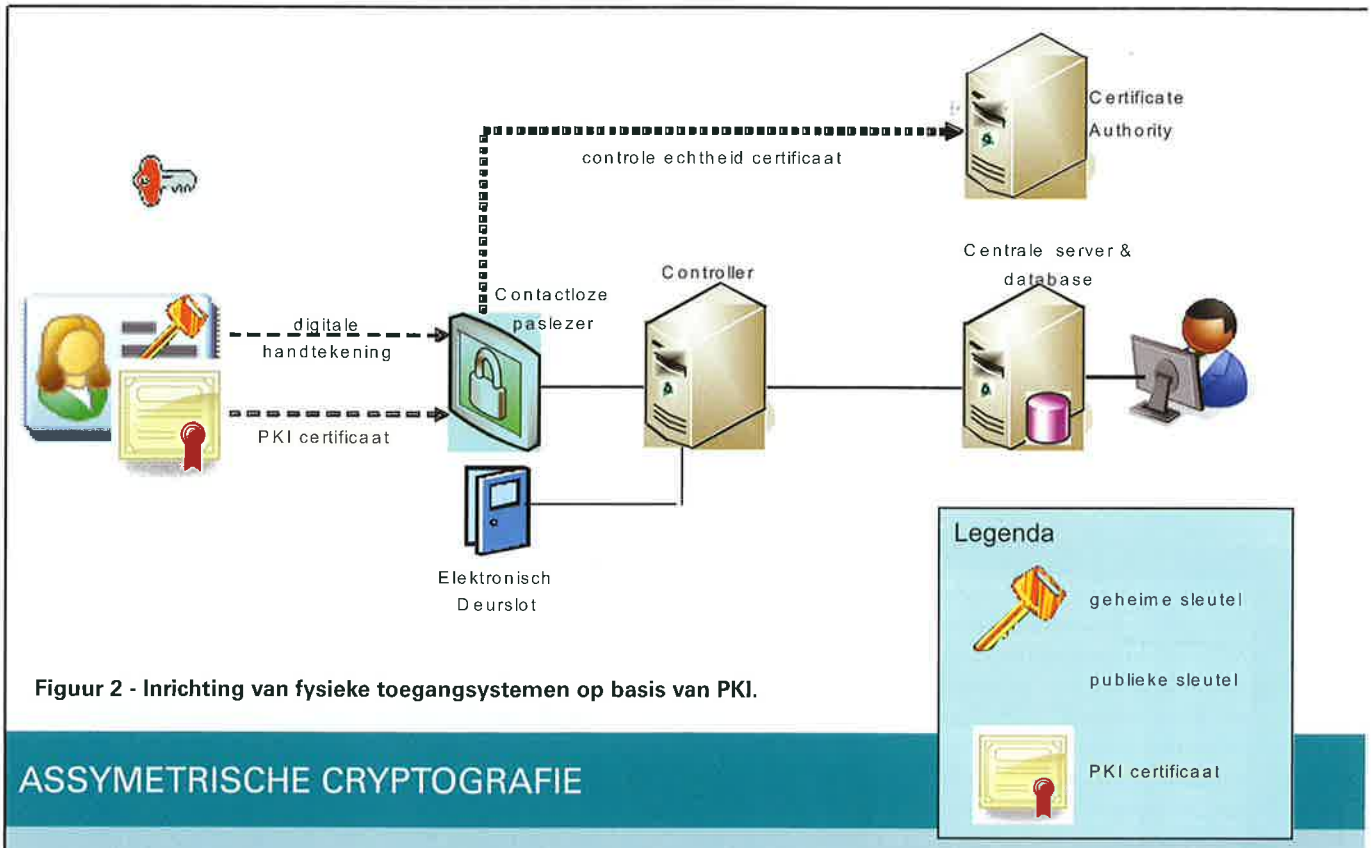


Figuur 1 - Traditionele inrichting van fysieke toegangsystemen op basis van symmetrische cryptografie.

platform of een cryptografisch algoritme. PKI binnen fysieke toegangsystemen past goed in de trend waarbij meer en meer componenten gekoppeld worden door netwerken gebaseerd op het internetprotocol (IP). Wanneer een organisatie op het punt staat om de contactloze chip voor fysieke toegang te vervangen, bijvoorbeeld in geval van een Mifare Classic, zou gebruik van PKI sterk moeten worden overwogen, zeker wanneer de organisatie al PKI heeft ingericht voor logische toegang en/of digitale ondertekening.

■ Ir. Geert Kleinhuis en Dr.ir. Eddy Olk
Werkzaam bij TNO
Geert.Kleinhuis@tno.nl, Eddy.Olk@tno.nl

*1) Jaap-Henk Hoepman, Geert Kleinhuis; Two worlds, one smart card; In 4th European PKI Workshop: Theory and Practice, Lect. Not. Comp. Sci. 4582, pages 236-247, Mallorca, Spain, June 28-30 2007
*2) Zack Martin, Is cryptography the future of physical access control?, http://www.fips201.com/articles/2010/05/17/is-cryptography-the-future-of-physical-access-control
*3) FIPS Publication 201-1, Personal Identity Verification (PIV) of Federal Employees and Contractors, NIST, March 2006
*4) NIST Special Publication 800-116, A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS), NIST, November 2008
*5) FIPS Publication 201-2 Draft, Personal Identity Verification (PIV) of Federal Employees and Contractors DRAFT, NIST, March 2011
*6) ISO/IEC 7816-15:2004, Identification cards - Integrated circuit cards - Part 15: Cryptographic information application



Figuur 2 - Inrichting van fysieke toegangsystemen op basis van PKI.

ASSYMETRISCHE CRYPTOGRAFIE

Asymmetrische cryptografie maakt gebruik van een sleutelpaar dat bestaat uit een privésleutel en een publieke sleutel. De privésleutel dient geheim te blijven terwijl de publieke sleutel via een (openbaar) certificaat gepubliceerd wordt. Via een PKI (Public Key Infrastructure) wordt de publieke sleutel gekoppeld aan een persoon of organisatie. (*7 en *8). Een CA (Certificate Authority) geeft een certificaat uit nadat de koppeling tussen publieke sleutel en sleutelhouder is gecontroleerd door een RA (Registration Authority). Door de PKI is het mogelijk om een digitale handtekening te controleren of informatie te versleutelen die alleen door de houder van de privésleutel kan worden ontsleuteld. PKI voorziet ook in de mechanismen Certificate Revocation List (CRL) (*9) en Online Certificate Status Protocol (OCSP) (*10) om de geldigheid van certificaten te controleren. Een certificaat wordt uitgegeven met een zekere geldigheidsduur (bijvoorbeeld vijf jaar), maar kan voortijdig worden ingetrokken als bijvoorbeeld vermoed wordt dat een privésleutel gecompromitteerd is.

*7) Carlisle Adams, Steve Lloyd, Understanding Public-Key Infrastructure - Concepts, Standards, and Deployment Considerations, Addison-Wesley Professional, 2002
*8) Russ Housley, Tim Polk, Planning for PKI, Wiley, 2001
*9) D. Cooper e.o., Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, http://tools.ietf.org/html/rfc5280
*10) M. Myers e.o., X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP, http://tools.ietf.org/html/rfc2560