



O Uso de Cartões Inteligentes para Acesso Físico Seguro

Um Informe da Smart Card Alliance Latin America

Data de Publicação: Julho 2003

Número de Publicação: ID-03003

Modificado em: Outubro 2006

Smart Card Alliance
191 Clarksville
Princeton Junction, NJ 08550
www.smartcardalliance.org
Telefone: 1-800-556-6828

Smart Card Alliance © 2003

Sobre a Smart Card Alliance Latin America (SCALA)

A Smart Card Alliance América Latina (SCALA por sua sigla em inglês) é uma associação sem fins de lucro, sem ideologia política, com múltiplos membros da indústria, líder em acelerar a aceitação em grande escala das múltiplas aplicações da tecnologia de cartões smart card. Os membros da Aliança incluem companhias líderes nos ramos bancário, serviços financeiros, computadores, telecomunicações, tecnologia, cuidados de saúde e indústrias de varejo e entretenimento, assim como inúmeras agências governamentais. Através de projetos específicos, tais como programas de educação, investigações de mercado, advocacia, relações industriais e foros abertos, SCALA mantém seus membros conectados aos líderes da indústria e a pensamentos inovadores. A Smart Card Alliance é a voz unificada da indústria de cartões smart card, sendo líder da discussão da indústria sobre o impacto e valor dos Cartões Smart Card nos Estados Unidos e na América Latina. Para maior informação, visite: www.smartcardalliance.org/latinamerica.

Direitos autorais © 2003 Smart Card Alliance, Inc. Todos os direitos reservados. A reprodução ou distribuição desta publicação em qualquer forma está proibida sem a autorização prévia da Smart Card Alliance. A Smart Card Alliance tem feito o seu maior esforço para assegurar que a informação descrita neste documento é preciso e correto na data da sua publicação, no entanto, não pode dar garantia do mesmo. A Smart Card Alliance não se responsabiliza pela precisão, integralidade ou adequação da informação deste informe.

Os membros da Smart Card Alliance: Os membros podem acessar todos os informes da Smart Card Alliance sem custo algum. Para informação sobre os direitos de reprodução e distribuição dos associados favor consultar a seção de ingressar à rede ou “Login” dos membros da Smart Card Alliance no seu “website”.

Agências de governo: Os empregados de governo podem pedir copias gratuitas deste informe contactando info@smartcardalliance.org ou afiliando-se a Smart Card Alliance como um Membro Governamental

Tabela de Conteúdo

Sobre a Smart Card Alliance Latin America (SCALA)	2
Tabela de Conteúdo	3
Resumo Executivo	4
Introdução	6
Visão geral de um Sistema de Controle de Acesso Físico	10
<i>Componentes do Sistema de Controle de Acesso</i>	10
<i>O Processo de Controle de Acesso</i>	11
A credencial de Identificação	12
O Leitor de Porta de Acesso	12
O Painel de Controle	13
O Servidor de controle de acesso	14
<i>Formato de dados para sistemas de controle de acesso</i>	14
<i>Raio de ação Operacional</i>	15
<i>Considerações de Seguridade</i>	15
Seguridade do cartão	16
Proteção dos dados	16
Autenticação do cartão e dos dados.....	17
Comunicações entre o cartão e o leitor do cartão	17
Comunicações entre o leitor de cartões e o painel de controle	17
<i>Implicações das Tendências Recentes na Arquitetura do Sistema</i>	18
O Cartão De Identificação Inteligente: O Papel Dos Cartões Inteligentes Nos Sistemas De Acesso Físico Seguro	19
Considerações Fundamentais Para A Implementação De Sistemas De Identificação De Acesso Físico Seguro	22
<i>Tecnologias de Cartões Inteligentes</i>	22
<i>Requerimentos e Problemas de Interface do Usuário</i>	24
<i>Considerações no Nível de Sistema</i>	25
<i>Administração do Ciclo de Vida</i>	28
<i>Custos e Benefícios</i>	30
<i>Tendências de Mercado</i>	31
Migração ao Sistema de Identidade de Acesso Físico com Base em Cartões Inteligentes	34
<i>Considerações chaves de migração</i>	34
Aplicações Permitidas Pelos Sistemas De Cartão Inteligente	38
<i>Aplicações de Controle de Acesso Lógico</i>	38
<i>Payment Support Suporte de Pagamento</i>	41
<i>Armazenamento Seguro de Dados</i>	42

Conclusão	44
Referências e Recursos	46
Reconhecimentos da Publicação.....	47
Apêndice A: Definição de Termos e Siglas	48
É um cartão sem contato que tem um circuito eletrônico que está desenhado para uma função específica (por exemplo, segurança, autenticação) sem um MCU integrado.	52

Resumo Executivo

Faz Sentido Usar Cartões Inteligentes para o Controle de Acesso Físico Seguro

Os cartões inteligentes estão sendo, crescentemente, aceitados como uma opção a escolher como credencial para o controle seguro de acesso físico. Os cartões de identificação com bases em padrões que podem ser usados para facilmente autenticar a identidade de uma pessoa, determinar um nível adequado de acesso e admitir fisicamente o portador do cartão a uma facilidade ou a uma determinada área física. Através do uso adequado da tecnologia de cartões inteligentes por contato ou sem contato no desenho geral de um sistema de acesso físico, profissionais de seguridade podem implementar as políticas de segurança mais fortes possíveis para qualquer situação.

Mais de uma aplicação de acesso pode ser desenvolvida num único cartão de identificação inteligente, permitindo aos usuários o acesso físico e recursos lógicos sem ter consigo múltiplas credenciais. A segurança pode modificar os direitos de acesso de forma dinâmica, dependendo do nível de

ameaça que for percebido, hora do dia ou qualquer outro parâmetro adequado. A tecnologia de informação (IT) pode registrar e atualizar os privilégios desde uma localização central. Os recursos humanos (HR) podem registrar os trabalhadores que entram e saem de forma rápida, dando ou retirando os direitos de acesso de uma vez em uma única transação. A organização como um todo incorre em custos de manutenção muito menores.

Os Critérios de Flexibilidade e Maturidade são os Aspectos de Maior Destaque da Tecnologia de Cartões Inteligentes

O apoio que dá o cartão inteligente a aplicações múltiplas permite às organizações expandir o uso do cartão para oferecer uma proposta de negócios muito convincente para a empresa. Os cartões inteligentes não só asseguram o acesso aos recursos físicos ou lógicos, eles também armazenam dados sobre o portador do cartão, pagam uma tarifa se for requerida, certificam transações e rastreiam as atividades do portador da identidade para propósitos de auditoria. Uma vez que os componentes de apoio ao sistema podem ser colocados em rede, as bases de dados compartilhadas e a comunicação entre computadores permitem que áreas funcionais separadas dentro de uma organização possam intercambiar e coordenar informação automaticamente, e instantaneamente distribuir informação exata através de grandes áreas geográficas.

A tecnologia de cartões inteligentes é com base em padrões maduros (por contato ou sem contato). Cartões que cumprem com esses padrões são desenvolvidos comercialmente e têm uma presença estabelecida no mercado. Vendedores múltiplos são capazes de apoiar componentes com bases em padrões necessários para implementar sistemas de acesso físico sem contato, oferecendo aos compradores com equipamento interoperativo e tecnologia a um preço competitivo.

A implementação deve ser guiada pelos requerimentos de aplicação e organizacionais

As organizações devem considerar muitos fatores quando vão implementar um novo sistema de controle de acesso físico, incluindo:

- Qual será a interface do usuário?
- Quais são os requerimentos de desempenho e de segurança necessários?
- Qual é o nível de integração requerido com outras aplicações da empresa?
- Como implementar uma arquitetura de sistema que, sendo custo-efetiva, alcance os requerimentos de segurança?
- Qual tecnologia deve ser utilizada para alcançar os requerimentos da organização?
- Como deve ser manejado o ciclo de vida da credencial de identidade?
- Como a organização migrará à nova tecnologia em quanto ainda se apoia nos sistemas de controle de acesso legados?

Os cartões inteligentes são flexíveis, e oferecem um dispositivo de migração de informação por meio do qual os requerimentos das organizações, e não a tecnologia do cartão em si, são as forças que dirigem o processo. Os cartões inteligentes de tecnologia múltipla podem reconhecer as tecnologias de controle de acesso legados, assim como incluir a nova tecnologia de chips com ou sem contatos. A migração de informação, quando planejada cuidadosamente, permite às organizações implementar novas funções, enquanto acomodam os sistemas legados na medida em que forem requeridos.

Sobre este informe

Este informe foi desenvolvido pela Smart Card Alliance para oferecer um documento primário sobre sistemas de acesso físico de identificação com base em cartões inteligentes. Este informe oferece respostas às perguntas, freqüentemente, feitas sobre o uso de cartões inteligentes para o acesso físico:

- Como funciona um sistema de controle de acesso físico?
- Que papel tem os cartões inteligentes nos sistemas de controle de acesso físico?
- Quais são os temas centrais que devem ser considerados quando se implementa um sistema de controle de acesso físico com base em cartões inteligentes?
- Quais outras aplicações podem ser combinadas com os sistemas de acesso físico com bases em cartões inteligentes?
- Quais são as opções de migração de informação para as organizações que estão migrando à sistemas de acesso físico com bases em cartões inteligentes?

Introdução

Gerenciar o acesso a recursos esta assumindo uma importância crescente para as organizações em todas as partes, desde pequenas companhias empresariais, até grandes empresas corporativas e corpos de governos de todos os níveis. Até a organização mais neutral, agora, reconhece o perigo de violações de seguridade.

A administração do acesso aos recursos significa controlar tanto o acesso físico como o acesso lógico, seja como esforços independentes ou através de uma abordagem integrado. O controle do acesso físico protege tanto os bens tangíveis, como intelectuais, de serem roubados ou de outra forma comprometidos. O controle do acesso lógico permite as empresas e organizações limitar o acesso aos dados, às redes, ou às estações de trabalho a aqueles que estão autorizados para ter o acesso.

Antecedentes

A coordenação de pessoas e privilégios tradicionalmente dependia do uso de um cartão de identidade como uma carteira de motorista, um cartão de biblioteca, um cartão de crédito, um cartão de associado ou um cartão de identificação do empregado. Tais cartões verificam a pessoa (p.ex: um guarda) ou a um aparelho (p.ex: um leitor eletrônico) de que o portador do cartão tem os direitos e privilégios em particular sinalados no cartão. Em resposta a necessidade de maior seguridade, a indústria desenvolveu tecnologias como a tira magnética, os códigos de barra e os circuitos de proximidade que podem ser incluídos em um cartão. O cartão pode então ser passado através de um leitor de tira magnética, esquadrinhado ou examinado por um leitor de código de barra ou apresentado a um leitor eletrônico com uma antena de frequência radial para a autorização automática de acesso. O número de identificação pessoal (PIN) pode ser ingressado através de um teclado para adicionar outro fator de autenticação que ajude a verificar que o portador do cartão é o dono do mesmo. No entanto, apesar de que estas tecnologias reduzem custos e aumentam a conveniência, eles não garantem que o usuário é de fato a pessoa autorizada.

Modificações na força de trabalho fazem mais críticos os problemas de identificar e autenticar indivíduos. Os dias de uma mão de obra estável e reconhecível estão, basicamente, passados. Atualmente, muitas corporações estão experimentando uma crescente rotatividade em seus empregados ou estão tendo dificuldades ao realizar tarefas específicas e, portanto, utilizam com maior frequência a contratantes ou empreiteiros externos. Este ambiente resulta na presença de pessoal novo e não reconhecido, que tem acesso aos bens corporativos e a informação corporativa. Apesar da alta rotatividade de empregados, geralmente, não é um problema sério para as organizações governamentais, a rotação de pessoal e o tamanho e complexidade de tais organizações criam uma situação similar com o potencial para que as pessoas não autorizadas possam ter acesso a recursos.

Portanto, o terreno está preparado para a introdução de sistemas de identificação de acesso com bases em um cartão de identidade ou outra credencial que inclui inteligência integrada. Tal credencial pode apoiar múltiplas aplicações seguras para processar informação de identificação pessoal, privilégios e direitos de acesso e incluir criptografia da informação. A aparição de uma credencial inteligente deu origem a um modelo completamente novo de controle de acesso que tem processamento rápido, autenticação pessoal e risco de migração. Este modelo representa um projeto para um sistema de identificação seguro, que resolve o problema fundamental do controle de acesso – como associar de forma veraz os indivíduos com seus direitos e privilégios no local onde a decisão de acesso deve ser tomada. Tal cartão de identidade inteligente pode incluir uma tira magnética, uma tira “*Wiegand*”, um código de barra, um aparelho de rádio frequência, um circuito de cartão inteligente e outras tecnologias de seguridade.

Sistemas de Controle de Acesso Físico com bases em Cartoes Inteligentes

Um sistema de controle de acesso físico é uma rede coordenada de cartões de identidade, leitores eletrônicos, base de dados especializados, software e computadores desenhados para monitorar e controlar o tráfico através de pontos de acesso.

Os sistemas de controle de acesso físico com base em cartões inteligentes são uma ferramenta de seguridade poderosa e eficiente para proteger os bens da empresa. A cada empregado se emite um cartão de identificação inteligente que contém a informação da empresa e os desenhos impressos para impedir a possibilidade de falsificação e para identificar o cartão como sendo um cartão oficial. O cartão tipicamente apresenta a foto do portador do cartão, cada cartão armazena informação protegida sobre a pessoa e os privilégios desta pessoa. Quando a pessoa se registra inicialmente e aceita o cartão, esses privilégios são colocados com precisão e seguridade através do sistema. (Se tais privilégios são modificados, a nova informação pode ser atualizada de forma imediata e segura através de toda a rede). Quando o cartão é colocado perto do leitor de cartão eletrônico, o acesso é dado de forma segura e precisa ou denegado a todos os espaços apropriados (por exemplo, um campus, uma garagem de estacionamento, um edifício em particular ou um escritório). Quando o empregado deixa a organização todos os privilégios de acesso físico são removidos de uma só vez. Toda tentativa futura dessa pessoa para reentrar a estes lugares usando um cartão expirado ou revocado podem ser denegadas e registradas automaticamente.

Tanto empresas privadas como agências de governo estão implementando, cada vez mais, sistemas de controle a acesso em base a cartões inteligentes. Breves perfis de implementações de cartões inteligentes estão incluídos no apêndice A, tais como SUN Microsystems, Microsoft, AmericanExpress e o Departamento de Estado dos Estados Unidos. Também incluído no apêndice A estão descrições de programas de cartões inteligentes planejados no Departamento de Seguridade dos Estados Unidos, da Administração Nacional de Aeronáutica Espacial (NASA), e da Administração de Seguridade do Transporte (TSA).

Oportunidades Adicionais

Idealmente, um sistema de controle de acesso oferece proteção tanto para acesso físico como lógico simultaneamente. A credencial usada para o acesso físico pode, também, realizar o acesso à rede de computadores e a infra-estrutura de chave pública – public key infrastructure (PKI) (incluindo o uso de acesso remoto seguro, e-mail seguro, assinatura digital e rede privada virtual segura – VPN -). A meta de proteção simultânea pode ser obtida por misturar ou compartilhar bases de dados seguras dedicadas a cada tipo de aplicação, abarcando o controle administrativo centralizado e a análise de tentativas de acesso não autorizadas. Ao combinar a informação de acompanhamento tanto dos sistemas físico como lógico, as políticas de seguridade podem ser, universalmente, introduzidas e investigadas. A informação recolhida pode ser inestimável na análise de risco a nível de toda a empresa.

A adoção de sistemas de controle de acesso em base a cartões inteligentes pode resultar em outras vantagens para uma organização, incluindo:

- Eliminação ou redução da necessidade de múltiplos cartões, PINs, códigos de acesso.
- A influencia dos sistemas legados, permitindo maior custo eficiência incluindo a reutilização de alguns componentes do sistema de acesso físico, ao mesmo tempo em que oferece um aumento significativo em seguridade.

-
- Eliminação da necessidade de repor cartões quando se modificam direitos e privilégios.
 - Administração centralizada, permitindo a organização a manter ou aumentar segurança ao mesmo tempo em que economiza tempo, conseguindo uma distribuição mais integral da informação, e administrando modificações globais para o acesso a privilégios desde um ponto único e redução das complexidades envolvidas em sistemas de sincronização múltipla.
 - Flexibilidade para apoiar funções múltiplas de uma organização (por exemplo, facilidades de segurança e IT) para administrar e controlar aplicações separadas num único cartão de identidade inteligente de aplicação múltipla.

Este informe oferece um documento base para entender os sistemas de controle de acesso físico que usam cartões de identificação inteligente para a identificação pessoal. O mesmo foi desenhado como um manual educativo para administrativos e planejadores de segurança, ele descreve a arquitetura e os componentes de um sistema de acesso físico, oferece uma guia sobre as considerações importante para a implementação deste sistema, descreve as tecnologias de cartões inteligentes usados para acesso físico e lógico, discute considerações ao migrar dos sistemas de acesso físico legados ao sistema com base em cartões inteligentes e mostra outras aplicações que podem ser combinadas com sistemas de acesso físico seguro com base a cartões inteligentes.

Visão geral de um Sistema de Controle de Acesso Físico

Para o usuário, um sistema de controle de acesso está composto por três elementos:

- Um cartão ou ficha (uma credencial de identidade) que é apresentada ao leitor de acesso na porta.
- Um leitor da porta de acesso, que indica se o cartão é válido e autoriza a entrada.
- Uma porta ou portão, que é destrancado quando se autoriza a entrada.

Detrás do cenário está uma rede complexa de dados, computadores e softwares que incorporam uma segurança mais forte. Essa seção descreve a operação e os componentes de um típico sistema de controle de acesso físico com base em cartões inteligentes. Isso oferece a informação para entender como as tecnologias de cartões inteligentes por contato e sem contato são usadas em aplicações de controle de acesso.

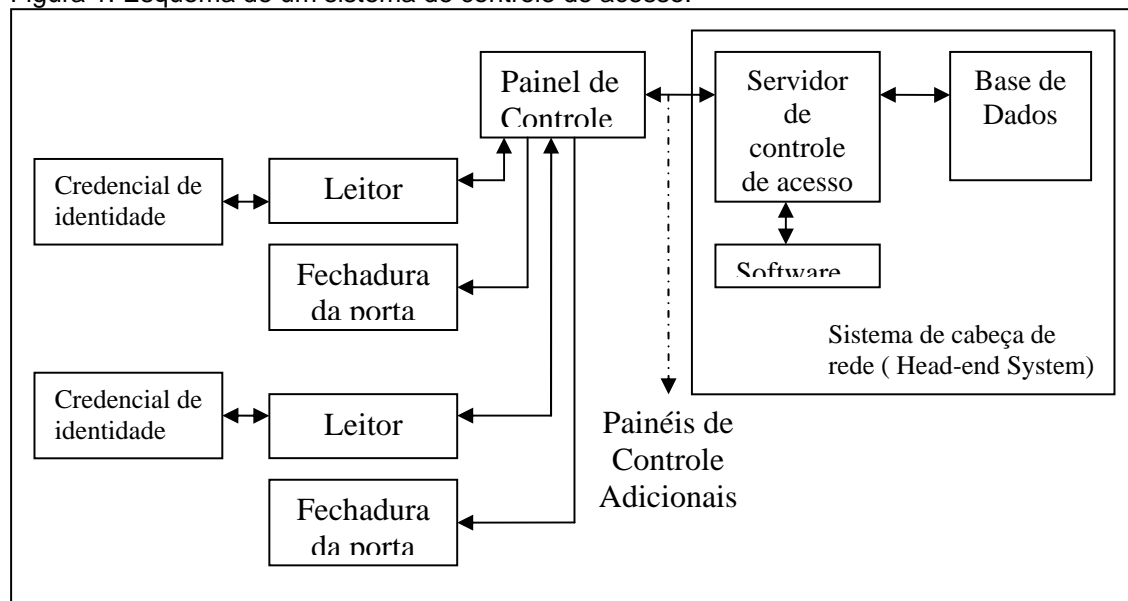
Componentes do Sistema de Controle de Acesso

Um sistema de controle de acesso típico tem os seguintes componentes:

- Uma credencial de identificação (cartão inteligente).
- Um leitor de porta de acesso (o leitor de cartão inteligente¹).
- Uma fechadura de porta.
- O painel de controle.
- Servidor de controle de acesso.
- O Programa ou o Software.
- Base de dados.

A figura 1 ilustra como estes componentes básicos estão interconectados. Cada componente será logo descrito nas próximas seções deste documento.

Figura 1: Esquema de um sistema de controle de acesso.



¹ Leitores de cartões inteligentes podem tanto ler como escrever ao cartão inteligente.
Smart Card Alliance © 2003

O Processo de Controle de Acesso

O processo de controle de acesso começa quando um usuário apresenta a credencial² (tipicamente a identificação ou a insígnia de cartão inteligente do empregado) ao leitor, que normalmente está localizado próximo à porta ou ao portal de entrada. O leitor extrai os dados do cartão, os processa e manda a informação ao painel de controle.

O painel de controle primeiro valida o leitor e logo aceita os dados transmitidos pelo leitor, o que acontece logo, depende se o sistema for centralizado ou descentralizado.

Num sistema centralizado, o painel de controle transmite os dados a um servidor de controle de acesso, e este compara os dados recebidos do cartão com a informação do usuário que está armazenada na base de dados. O programa de controle do acesso determina os privilégios e a autorização de acesso do usuário, a hora, a data e a porta de entrada, ou qualquer outra informação que a companhia possa requerer para assegurar a sua segurança. Quando o acesso é autorizado, o servidor de controle de acesso manda um sinal para o painel de controle para destrancar a porta. O painel de controle logo envia dois sinais: uma para a fechadura da porta adequada que destranca a porta, e outra para o leitor da porta de acesso, que emite um som audível ou outro sinal para o usuário para que ele entre.

Num sistema distribuído ou descentralizado, o painel de controle permite ou nega a entrada. O servidor de controle de acesso periodicamente oferece, aos painéis de controle, dados que habilitam o software do painel determinar se o acesso está ou não autorizado para o usuário. O painel de controle, então, realiza as funções, de servidor de controle de acesso, descritas acima e toma a decisão de permitir ou negar a entrada. Habilitar os painéis de controle a ter a função de decisão tem a vantagem de requerer menos comunicação entre os painéis de controle e o servidor de controle de acesso central, ademais de melhorar o desempenho e a confiabilidade do sistema.

Se uma função biométrica ou PIN é incorporada ao sistema, o leitor tipicamente autentica esse dado. A validade pode ser determinada pelo leitor ou dentro do cartão de identificação inteligente ao comparar os dados com o padrão biométrico ou com o PIN que está armazenado no cartão. (Em alguns casos, o dado biométrico pode ser enviado ao painel de controle para o processamento). Se a informação adicional é válida, o leitor envia o número de identificação da credencial para o painel de controle. Se a informação não é válida, então, o leitor de cartão indica que a entrada é negada.

A resposta a um cartão não válido é definida pela política de segurança da companhia e pelos seus procedimentos. O servidor de controle de acesso ou o painel de controle poderia ignorar os dados e não enviar um código de destrancar ao controlador ou a fechadura da porta. Ele poderia enviar um sinal que faz que o leitor emita um som diferente indicando que o acesso foi negado, o qual poderia notificar ou ativar outros sistemas de segurança (televisão de circuito fechado, alarmes), indicando que um cartão não autorizado está sendo apresentado ao sistema.

² Este informe usa o termo “credencial” para referir-se ao aparelho de identificação geral (tanto o aparelho físico como os dados que ele contém). Normalmente se refere a isso como a “ficha de identificação” nos sistemas de controle de acesso físico.

Cada componente do sistema de controle de acesso neste processo é descrito em maior detalhe a continuação.

A credencial de Identificação

Uma grande variedade de diferentes tecnologias de identificação está atualmente sendo usada para controle de acesso: tiras magnéticas, tiras Wiegand, “barion ferrite”, tecnologia de proximidade de 125 Khertz³, cartões inteligentes de contato e sem contato. Essas tecnologias podem ser empacotadas em uma grande variedade de formatos – qualquer coisa desde chaves de bolso ou um crachá de empregado ou até formas mais exóticas, como um relógio de pulso ou um anel. No entanto, todas as credencias operam, basicamente, da mesma forma: elas guardam dados que autenticam a credencial e/ o usuário.

Algumas tecnologias de credencial são para ler unicamente. A informação está registrada permanentemente na credencial, e quando este se expõe ao leitor, a informação é enviada ao sistema. Esse tipo de credencial somente valida se a informação mesma é autêntica. Mas não confirma que a pessoa que está apresentando a credencial é a pessoa autorizada a ter a posse da mesma, ou que a credencial em si é genuína.

A tecnologia de cartões inteligentes por contato definida pelo ISO-IEC 7816 e a tecnologia de cartões inteligentes sem contato definida pelo ISO-IEC 14443 e o ISO-IEC 15693 tem capacidade tanto para ler e escrever quanto para armazenar dados. Os credenciais que usam essas tecnologias são dispositivos inteligentes. Eles podem armazenar privilégios, autorizações e registros de assistência. Eles podem armazenar PINS e padrões biométricos, oferecendo uma capacidade de autenticação de dois ou três fatores simultâneos. A credencial já não é apenas uma portadora de um número único, mas é também uma portadora segura e portátil de dados ao mesmo tempo.

O Leitor de Porta de Acesso

O leitor de porta de acesso pode ter uma ou mais interfases, acomodando algum tipo de combinação de cartões inteligentes de contato ou sem contato, incluindo um teclado para o PIN e um leitor biométrico. Como o leitor responde depende do tipo de credencial apresentada e a política de seguridade da organização.

Quando o leitor é usado com cartões inteligentes sem contato, ele atua como um pequeno rádio de baixa potência, transmissor e receptor, constantemente transmitindo um campo de rádio frequência (RF) ou um campo eletromagnético chamado campo de recepção (EXCITE FIELD). Quando o cartão sem contato está dentro do alcance do campo de recepção, a antena interna do cartão converte a energia de campo numa eletricidade que ativa o chip no cartão. O chip então usa a antena para transmitir dados ao leitor.

Quando o leitor é usado com um cartão inteligente de contato, o leitor inclui uma abertura que contém um conector para o cartão inteligente. O cartão e o conector no leitor devem estabelecer contato físico.

³ A tecnologia de proximidade de 125 kHz é geralmente referida como “prox” (em inglês).
Smart Card Alliance © 2003

Os leitores de acesso que incluem um teclado para o número de identificação pessoal (PIN) e um leitor biométrico (tipicamente uma impressão digital ou um leitor geométrico da mão) normalmente apóiam uma autenticação de dois ou três fatores simultâneos se for requerido. Por exemplo, um estabelecimento pode requerer somente a apresentação do cartão sem contato quando o risco de seguridade é baixo, mas requerer dados biométricos, também, quando aumenta o nível de ameaça. Quando o risco de seguridade é alto, pode ser necessário apresentar o cartão inteligente de contato e usar o leitor biométrico e o teclado para introduzir o PIN. Esses leitores de múltiplos fatores podem ser usados quando forem desejáveis para variar os insumos requeridos durante o dia, por dia da semana ou por localização. Os requerimentos para fatores de autenticação adicional podem ser estabelecidos pelas políticas de seguridade da organização.

Quando o leitor já recebeu todos os dados requeridos, ele tipicamente processa a informação em uma das duas possíveis formas: ou a informação é enviada imediatamente ao painel de controle, ou o leitor analisa os dados antes de enviá-los ao painel de controle. Ambos os métodos são amplamente utilizados. Cada um tem suas vantagens e desvantagens.

Os leitores mais simples enviam os dados diretamente ao painel de controle. Esses leitores não fazem nada para avaliar os dados ou a legitimidade da credencial. Esses leitores são tipicamente leitores de um único fator ou são genéricos, desta forma, eles podem ser colocados no inventário, e facilmente adicionados ou retirados do sistema de controle de acesso.

Os leitores que analisam os dados devem ser integrados ao sistema de controle de acesso, isto é, eles devem interpretar e manipular os dados enviados pelo cartão são então transmitir os dados numa forma que seja usável pelo painel de controle. Tal sistema pode oferecer um nível de seguridade muito maior. O leitor pode determinar a legitimidade do cartão (e o cartão pode determinar a legitimidade do leitor), comparar os dados biométricos ou a entrada do PIN, e manipular os dados da credencial de tal forma que a informação que o leitor envia ao painel de controle não é a mesma daquela que foi lida do cartão. O processo de autenticação do cartão ao leitor e do leitor ao cartão é chamado autenticação mútua, e o mesmo constitui uma das vantagens principais de um sistema com base em cartões inteligentes.

O Painel de Controle

O painel de controle (frequentemente referido como o controlador ou simplesmente o painel) é o ponto de comunicação central para o sistema de controle de acesso. Tipicamente, o painel supre de poder e estabelece interface com múltiplos leitores em diferentes pontos de acesso. O controlador se conecta a fechadura eletromecânica da porta requerida para destrancar fisicamente a porta ou ao mecanismo de destranque para um portal de entrada (tal como um portão de estilo giratório, de estacionamento, ou um elevador). Ele pode ser conectado a diferentes alarmas: sirenas, digitadores automáticos, luzes. E por fim, o painel de controle geralmente está conectado a um servidor de controle de acesso.

Dependendo do desenho do sistema, o painel de controle pode processar dados do leitor de cartão e do servidor de controle de acesso e tomar uma decisão final sobre a autorização, ou ele pode passar os dados a um servidor de controle de acesso para que este então tome a decisão.

Normalmente o painel de controle toma a decisão de destrancar a porta e passa o dado da transação ao computador principal e o sinal de destrancar para o leitor. É importante que o painel de controle (Vs. o leitor) seja o que gere o sinal de destrancar, já que o painel de controle está localizado dentro do estabelecimento ou em um quarto seguro, enquanto o leitor do cartão está localizado em uma área aberta ou insegura.

Em conclusão, o painel de controle armazena informação de formato dos dados. Essa informação identifica que porção do fluxo de dados recebidos do cartão é usada para tomar as decisões de controle de acesso. Os cartões e os leitores implementados com tecnologias diferentes podem intercambiar dados em diferentes formatos. No entanto, o painel de controle precisa saber como interpretar e processar esses dados, por exemplo, se um leitor envia 35 bits de dados e o painel está desenhado para ler somente 16 bits, o painel deve ou rejeitar os dados ou truncar nove bits. O formato de dados controla como o painel interpreta os dados recebidos.

O Servidor de controle de acesso

O sistema de cabeça de rede ("head-end system") também referido como o sistema de fundo ("back-end system") ou sistema principal ("host system") inclui o servidor de controle de acesso, o software e a base de dados. A base de dados contém informação atualizada sobre os direitos de acesso dos usuários.

Num sistema centralizado, o servidor de controle de acesso recebe os dados do cartão do painel de controle. O programa correlaciona os dados do cartão com os dados na base de dados, determina os privilégios de acesso da pessoa, e indica se a pessoa pode ser admitida. Por exemplo, se a uma pessoa se permite entrar ao edifício somente entre as 8 AM e as 5 PM e são as 07h45min da manhã, ela não será admitida. No entanto, se são 08h01min AM, o computador deve responder ao painel de controle, indicando que a porta pode ser destrancada.

A maioria dos sistemas é descentralizada. Nos sistemas descentralizados, o servidor de controle de acesso periodicamente envia informação de controle de acesso atualizada aos painéis de controle, e lhes permitem operar independentemente, tomando a decisão de autorização para a credencial apresentada com base nos dados armazenados no painel.

As características operacionais nos sistemas centralizados ou descentralizados são determinadas em função dos requerimentos específicos de controle de acesso da organização que está implementando o sistema.

Formato de dados para sistemas de controle de acesso

O formato de dados para os sistemas de controle de acesso é um elemento crítico do desenho. O formato dos dados se refere ao padrão de bits que o leitor transmite ao painel de controle. O formato especifica quantos bits tomará o fluxo de dados e quantos bits isto representa. Por exemplo, os primeiros bits podem representar o código do estabelecimento, os próximos bits, um número de identificação de credencial único, o próximo pode ser de paridade e assim por diante.

Muitos vendedores de sistema de controle de acesso desenvolveram os

seus próprios formatos, fazendo com que os códigos de cada vendedor sejam únicos. Como os padrões dos dentes de uma chave de porta, os formatos se mantêm em segredo para prevenir que uma pessoa ou companhia não autorizada possam duplicar o cartão. Os formatos dos sistemas de controle de acesso atualmente instalados devem ser tomados em conta quando se estão definindo os requerimentos para a implementação de novas tecnologias de sistemas de controle de acesso físico.

Raio de ação Operacional

A distância do leitor na qual a credencial é efetiva (chamado raio de ação operacional) é uma característica importante do sistema de controle de acesso. Essa característica pode afetar a percepção do usuário final com respeito à conveniência do uso do sistema. Para sistemas utilizando cartões inteligentes de contato, o raio de ação operacional não constitui um obstáculo, já que os cartões são inseridos no leitor e o contato físico é realizado.

O raio de ação operacional é determinado por muitos fatores, incluindo tanto as especificações do desenho do sistema e o ambiente no qual o leitor é colocado. Os fatores que afetam o alcance de operação incluem a forma da antena, o número de voltas que tem a antena, o material da antena, os materiais que estão ao redor da antena, a orientação da credencial em relação ao leitor, os parâmetros elétricos do chip, as características contra colisão e a força do campo do leitor. Organizações governamentais (como a UFCC, a UL e a CE) estão envolvidas na aprovação ou em especificar os estágios de frequência ou os limites do poder de transmissão. O alcance de transmissão pode ser aumentado fortalecendo a antena (p.ex.: aumentando o número de espirais da antena, o tamanho da antena ou o poder transmitido pela antena).

A localização do leitor pode afetar o alcance de operação de um leitor sem contato. Por exemplo, a proximidade do leitor ao metal pode modificar o campo de recepção ou inclusive servir de escudo entre o leitor e o cartão. Assim que um leitor posto sobre uma placa de metal sólida, próxima a uma porta de metal ou envolta num compartimento de metal (para protegê-lo de vandalismos), pode ter um alcance de transmissão curto.

O alcance de operação da credencial de identificação para qualquer uma das tecnologias sem contato é uma decisão crítica do desenho para um sistema de controle de acesso físico. O alcance de transmissão apropriado será determinado conforme as políticas de seguridade da organização, a estrutura de segurança e os seus requerimentos.

Considerações de Seguridade

Para aliviar os riscos de acesso não autorizado ou de ataques deliberados, a segurança de todo o sistema de controle de acesso deve ser considerada. Isso começa com o processo inicial de emissão do cartão e inclui os componentes do sistema (tais como a rede, a bases de dados, o software, hardware, câmeras, leitores, cartões), processos do sistema (p.ex.: os procedimentos do guarda de segurança) e a proteção dos dados dentro dos componentes do sistema e durante sua transmissão. O desenho do sistema considerará quais características de seguridade precisam ser

implementadas dado o ambiente do sistema e a probabilidade real de um ataque.

Seguridade do cartão

Os cartões inteligentes podem ajudar a deter a falsificação, impedir a manipulação com o cartão de identidade e evitar o uso de um cartão não autorizado. Os cartões inteligentes incluem uma variedade de capacidades tanto de hardware como de software, que detectam e reagem às tentativas de manipulação, e ajudam a conter possíveis ataques, incluindo: a voltagem, a frequência, sensores de luz e de temperatura; filtros de relógios; memória embaralhada; fontes de energia constante; e desenhos de chips para resistir às análises por inspeção visual, micro-sondagem ou manipulação de chip. Nos lugares onde os cartões de identificação inteligente serão usados para a verificação manual de identidade, características de seguridade podem ser adicionadas ao corpo do cartão inteligente, tal como caracteres únicos, combinações de tintas a cores ou multicores, micro-impressões, tinta ultravioleta de alta qualidade, imagem fantasma pela (uma fotografia secundária do portador numa localização alternativa no cartão), hologramas de múltiplos níveis e imagens tridimensionais⁴.

Quando desenhados e implementados de forma adequada, os cartões inteligentes são quase impossíveis de falsificar ou de duplicar, e os dados contidos no chip não podem ser modificados sem a devida autorização (p.ex.: com as senhas, autenticação biométrica ou chaves de acesso criptográfico). Na medida em que as implementações do sistema tenham uma política de seguridade efetiva e incorporem os serviços de segurança necessários oferecidos pelos cartões inteligentes, tanto as organizações como os portadores de identidade podem ter um alto grau de confiança na integridade da informação de identidade, e no seu uso autorizado de forma segura.

Proteção dos dados

Um dos argumentos mais fortes para o uso de sistemas, com base no uso de cartões inteligentes para controle de acesso físico, é a capacidade de usar dados misturados ou criptográficos para proteger a informação tanto no chip como durante a transmissão. A seguridade e a confiabilidade da informação requerida para identificar os indivíduos, seus direitos e privilégios, é uma questão-chave para o sucesso de um sistema de controle de acesso físico.

Os cartões inteligentes suportam algoritmos criptográficos simétricos⁵, que asseguram proteção substancial e tempos excelentes de processamento. A criptografia de chave simétrica é amplamente usada para o controle de acesso físico, e usa a mesma chave para criptografar e decifrar, fazendo-o extremamente rápido e confiável. Quando um sistema de controle de acesso inclui acesso lógico e privilégios PKI, e quando o tempo de processamento não é uma questão importante, os algoritmos criptográficos assimétricos podem ser usados⁶. Chaves múltiplas podem ser armazenadas

⁴ Informe do grande jurado em nível de estado: roubo de identidade na Flórida.

⁵ Os algoritmos de chave simétrica mais comumente usados atualmente utilizam DES (Data Encryption Standard), Triple DES (seja em um formato de dois ou três fatores, IDEA (International Data Encryption Standard), AES Advanced Encryption Standard) e MIFARE.

⁶ algoritmos criptográficos assimétricos mais comumente usados são RSA, ECC (Elliptic Curve Cryptography) e DSA (Digital Signature Algorithm).

num único chip para atender aos requerimentos de seguridade para o uso em aplicações múltiplas, fornecendo assim melhor seguridade para a complexidade crescente dos sistemas de hoje.

Autenticação do cartão e dos dados

Um sistema de acesso físico seguro deve ter a garantia imparcial que tanto o cartão de identificação apresentado ao leitor como os dados contidos no mesmo são autênticos. Em alguns casos, é importante verificar que o leitor também é autêntico (como determinado pelo cartão) para prevenir o uso de terminais de falsificação para extrair dados.

Aparte do uso de um PIN e/ou um sistema biométrico que ativa o cartão ou autentica a pessoa, os cartões inteligentes têm a capacidade única de oferecer características de autenticação interna com bases no chip que usam mecanismos de criptografia simétrica ou assimétrica para oferecer soluções altamente confiáveis, para demonstrar que o cartão e os dados são genuínos. Para a autenticação segura do cartão, os cartões inteligentes tem a habilidade única de usar técnicas criptográficas ativas para responder a um sinal que solicita uma senha do leitor para provar que o cartão possui um segredo que pode autenticar a validade do cartão.

Comunicações entre o cartão e o leitor do cartão

Como em qualquer processo que envolve sinais eletrônicos, os dados transmitidos através dos componentes deve ser monitorado. Essa possibilidade deve ser considerada no desenho de seguridade interno do seu ambiente (p.ex., se a área está em observação ou se alguém poderia introduzir fisicamente outro dispositivo ou colocar um dispositivo de monitoria dentro do raio de ação do sinal) e a probabilidade real de que tal ataque ou esforço se leve a cabo.

Dependendo do ambiente e do perfil de risco, uma organização pode estar preocupada de que os dados enviados a cartões de identificação de contato ou sem contato ao leitor do cartão possam estar sendo monitorados, permitindo que se realize uma entrada ilegal caso um cartão ou um dispositivo furtivo possa duplicar os dados. Os cartões inteligentes respaldam as técnicas de criptografia e de seguridade padronizadas ao nível da indústria, que estabelecem uma comunicação segura entre o cartão e o leitor, e ao mesmo tempo habilitam métodos de autenticação do cartão e do leitor.

As chaves de seguridade usadas tanto para a criptografia como a autenticação são mantidos em fichas seguras (módulos de cartões inteligentes), tanto no cartão como no leitor, e são altamente resistentes a qualquer ataque.

Comunicações entre o leitor de cartões e o painel de controle

Quando um ponto de acesso está num lugar que não pode ser observado ou que não tem os cabos fisicamente seguros, as organizações podem estar preocupadas de que um intruso pudesse remover o leitor do cartão do seu lugar e ler o fluxo de dados enviados ao painel de controle, ou colocar um computador pessoal ou outro dispositivo nestes fios e mimetizar a inserção de um cartão válido para obter autorização. A maioria dos leitores de cartão atualmente transmitem dados para o painel de controle usando um dos dois formatos possíveis: Wiegand ou tira magnética. O formato Wiegand usa duas linhas de sinais: D0 para a transmissão de pulsos de dados zero e D1

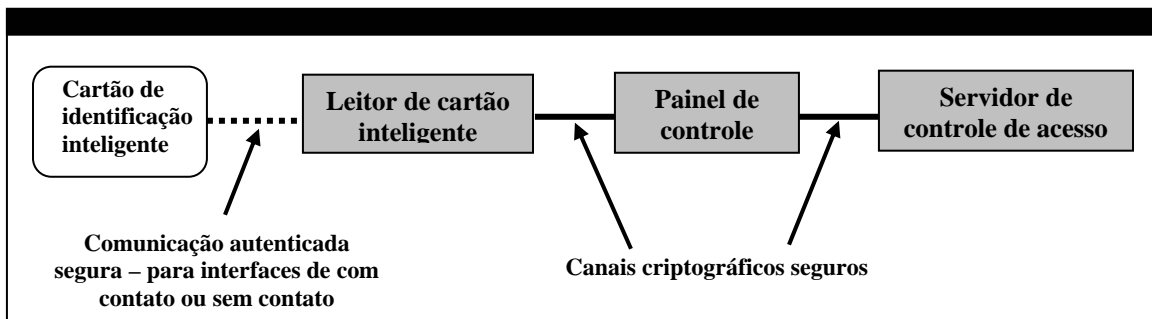
para transmitir pulsos de dados 1. O formato de tiras magnéticas utiliza duas linhas de sinais – um para dados e outro para o relógio. Estas cadeias de dados não são consideradas seguras.

Ao oferecer um canal seguro do cartão ao leitor e do leitor ao painel de controle se supera esta ameaça potencial à seguridade. Ao oferecer canais seguros se neutraliza a maioria das ameaças sérias porque o leitor e o cartão são os dois elementos que estão expostos e fisicamente disponíveis ao atacante.

O canal de comunicação do leitor ao painel de controle pode ser assegurado de uma forma similar a que se usa para assegurar o canal entre o cartão e o leitor. A troca de dados entre os dois dispositivos pode ser cifrada para máxima seguridade e o leitor e o painel podem ser autenticados durante a transação.

Devido a que a conexão entre o painel de controle e o sistema de controle de acesso é interno, em um edifício, ou localizado em um quarto seguro, geralmente não é tão susceptível de ser atacada. No entanto, esta conexão pode ser assegurada usando as técnicas descritas nessa seção para que todo o sistema tenha um canal de dados seguros de ponta a ponta. A figura 2 ilustra um exemplo de como um sistema de controle de acesso físico com base em cartões inteligentes pode oferecer uma seguridade de ponta a ponta.

Figura 2: Exemplo de um Sistema de Seguridade de Ponta a Ponta em um Sistema de Acesso Físico Com base em Cartões Inteligentes



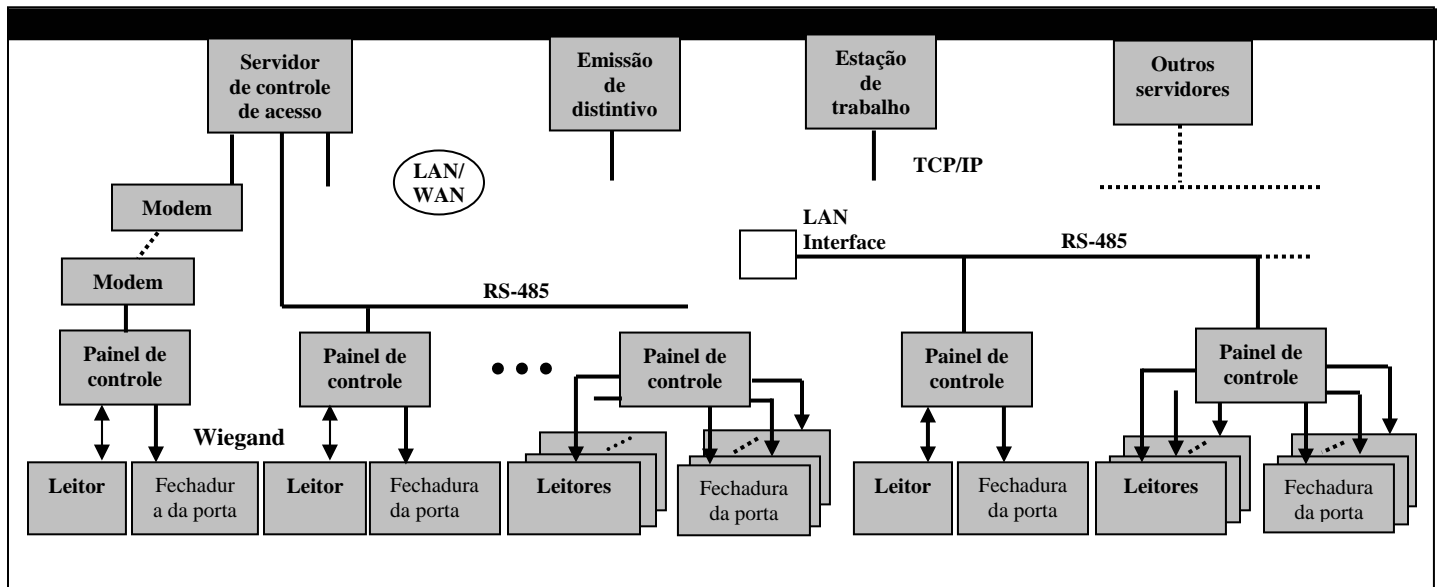
Implicações das Tendências Recentes na Arquitetura do Sistema

Tradicionalmente, os sistemas de controle de acesso físico eram controlados pelo departamento de seguridade corporativa. No entanto, com a aparição de sistemas centrados em redes com base na tecnologia de internet e TCP/IP, os sistemas de controle de acesso evoluíram a sistemas de rede que combinam muitas funções e envolvem múltiplos departamentos. Os sistemas modernos, ademais das funções de controle de acesso, incluem também funções corporativas tais como, gerenciamento de credenciais e as bases de dados dos funcionários. Os sistemas de controle de acesso por rede ainda não chegaram a alcançar os seus limites de funcionalidade: é fácil conceber que um leitor de cartões atue como um relógio de tempo, desta forma, estendendo o sistema aos departamentos de recursos

humanos e de pagos (figura 3), ou um cartão de identificação que inclui uma aplicação de pagamento para o sistema de trânsito local.

Estas aplicações múltiplas novas requerem uma arquitetura em rede com o envolvimento e a cooperação de departamentos como segurança, IT, recursos humanos, e outros, para a implementação de um sistema de controle de acesso físico corporativo.

Figura 3: Exemplo de um Sistema de Controle de Acesso Físico em Rede



O Cartão De Identificação Inteligente: O Papel Dos Cartões Inteligentes Nos Sistemas De Acesso Físico Seguro

Originalmente, o distintivo do empregado era usado como uma credencial de identidade visual. O acesso aos edifícios e portas era dado quando um guarda reconhecia o distintivo do portador do cartão. Tecnologias para automatizar o controle de acesso (tais como tiras magnéticas, códigos de barras e chips de proximidade) foram desenvolvidas para reduzir os custos operacionais, melhorar a segurança, e incrementar a conveniência.

Se bem é certo que estas tecnologias reduzem os custos operacionais e aumentam a conveniência, elas não garantem que o portador do crachá é de fato a pessoa autorizada a portar o mesmo. Tecnologias de identificação mais antigas oferecem uma segurança mínima ou nula para redes de computação. O requerimento de uma credencial única e segura para acesso lógico e físico, e para proteger a informação privada do individuo levaram a emergência do cartão de identificação inteligente: uma credencial de identificação na quais as tecnologias de cartões inteligentes por contato e/ou sem contato estão integradas a uma identificação corporativa que permite que os sistemas de acesso sejam implementados com níveis adicionais de segurança – autenticação, autorização e admissão.

O cartão de identificação inteligente oferece à pessoa (ou dispositivo) um acesso seguro, autenticado tanto aos recursos físicos como virtuais. O crachá pode autorizar acesso aos edifícios, às redes de computadores, aos arquivos de dados ou ao computador pessoal do usuário. Além do mais, estes mesmos cartões podem agora incluir aplicações que permitem acesso a sistemas de transporte de massas, contas de pagamentos e outros dados seguros. O denominador comum de todas essas aplicações é o requerimento de autenticação do usuário.

Muitas das pessoas envolvidas na compra, implementação e uso de cartões de identificação inteligentes – desde o diretor executivo (CEO) até (e mais importante) o empregado – se estão dando conta dos benefícios dos cartões. Quase todas as revistas sobre seguridade incluem pelo menos um artigo sobre a convergência de acesso físico e lógico. Tais escritos descrevem as vantagens de seguridade, ROI, conveniência e considerações de implementação.

Os Benefícios do Cartão de Identificação Inteligente

Ao escolher uma credencial de acesso se devem atender as preocupações de uma série de áreas funcionais de uma organização. As necessidades da gerência executiva para assegurar tanto o acesso físico como as redes com orçamentos operativos cada vez menores, os diretores executivos e os oficiais chefes de finanças estão demandando um forte caso de negócios para soluções que sejam mais custo-efetivo. O oficial chefe de segurança (CSO) e o oficial chefe de informática (CIO) precisam ser notificados rapidamente sobre qualquer rompimento do esquema de segurança, identificar e localizar o perpetrador e recolher toda evidência forense que possa ser usada em corte. O departamento de recursos humanos quer que os novos empregados comecem a render desde que são contratados, aumentando a eficiência e o lucro. A legislação governamental demanda que se respeite à privacidade das pessoas e que, finalmente, os empregados tenham credencial de identificação fácil e conveniente de ser usada. De outra forma, ou os empregados buscarão formas de esquivar a segurança, ou os custos do credenciamento do empregado aumentarão de forma tão significativa que a companhia terminará abandonando o sistema.

Os cartões de identificação inteligentes são uma solução custo-efetiva e flexível que atendem aos requerimentos de toda a organização. Um único cartão de identificação inteligente pode incorporar múltiplas tecnologias, acomodando tanto os sistemas de controle de acesso novos como os já existentes, como parte de um plano geral de migração às novas tecnologias de controle de acesso. Os crachás para os empregados podem apoiar uma ampla gama de perfis de seguridade dependendo do nível de acesso requerido pelo empregado. Por exemplo, alguns crachás podem oferecer apenas acesso limitado às instalações e redes, enquanto que outros podem oferecer acesso especial a áreas restringidas, e usar chips de cartões inteligentes por ou sem contato para apoiar padrões biométricos que autenticam o usuário do cartão; algoritmos com senhas seguras que autenticam o cartão e o leitor um ao outro; e um protocolo seguro de gerenciamento do sistema que é modificado cada vez que o crachá é apresentado a um leitor para prevenir a duplicação do cartão e proteger a sua informação.

As novas especificações e produtos tanto em software, como em integração de sistemas ajudam para a identificação e a análise de violação de seguridade. Ao vincular o acesso físico e as bases de dados de IT, sô oferece o potencial de que atividades suspeitas possam ser identificadas imediatamente. Por exemplo, se um computador é acessado por um empregado que já abandonou o edifício do departamento de IT, pode ser notificado imediatamente e investigar a atividade. Da mesma forma, os seguranças podem ser notificados se um computador de uma área restringida for acessado por um empregado que não está autorizado para estar em essa área. As comunicações entre os sistemas de acesso físico e lógico permitem as companhias protegerem dados confidenciais e os temas de segurança da identidade.

Sistemas de controle de acesso devem atender as necessidades do empregador e do empregado e, também, os requerimentos legais. Os cartões de identificação inteligentes estão disponíveis para usar os protocolos mais avançados e as técnicas de prevenção contra sondagem. Conseqüentemente, a informação de um empregado somente está disponível para partícipes a quem o empregador autorizou o acesso. Uma organização pode requerer usar um único processo para manejar as autorizações, acessos e privilegio de um empregado. A vinculação de recursos humanos, informática e bases de dados de acesso físico significa que o empregado pode fazer uma só viagem ao departamento para receber um crachá que contenha toda a informação requerida. A base de dados de recursos humanos (RH) pode indicar quais são os privilégios de acesso necessários para serem designados. O software de TI pode verificar a base de dados de recursos humanos (RH) e designar as senhas e os certificados requeridos. Uma impressão digital biométrica e uma foto digital podem ser tomadas. Com essa informação, um cartão em branco pode logo ser inserido dentro da impressora do crachá, e toda a informação requerida descarregada ao cartão, podendo então ser impresso. O empregado recebe o crachá em questão de minutos e começa a trabalhar imediatamente.

Os cartões de identificação inteligentes são convenientes e fáceis de usar. Os empregados têm apenas um crachá que manter, reduzindo assim a probabilidade de perder, esquecer ou estragar o crachá. Os empregados não precisam agarrar, desajeitadamente, o crachá para encontrar o correto ou sentir que estão levando consigo um baralho de cartas.

Conclusão

Os governos, as corporações e universidades estão descobrindo que o cartão de identificação inteligente pode atender suas necessidades tanto de aplicações de acesso físico como de acesso lógico. Um sistema com base em cartões inteligentes oferece benefícios a toda organização, melhorando a segurança e a conveniência para o usuário, ao mesmo tempo reduzindo os custos administrativos e de gestão. A tecnologia de cartão inteligente oferece uma plataforma flexível, de baixo custo não só para o controle de acesso físico, mas também para novas aplicações e processos que podem trazer benefícios como um todo.

Considerações Fundamentais Para A Implementação De Sistemas De Identificação De Acesso Físico Seguro

A implementação de sistemas de identificação de acesso físico com base a cartões inteligentes seguros requer a consideração de vários aspectos centrais, começando pela consideração cuidadosa e o análise dos requerimentos operacionais.

Tecnologias de Cartões Inteligentes

Quando se considera a implementação de um novo sistema de acesso físico seguro, há duas soluções ao problema de como a aplicação de segurança física lê a credencial: por contato ou sem contato. A decisão de adotar a tecnologia de cartões inteligentes com contato ou sem contato depende dos requerimentos da organização.

Tecnologia de Cartões Inteligentes Sem Contato

Esta tecnologia é mais adequada para acesso físico através de portais de alto tráfego ou de portas, sendo a melhor escolha para áreas onde o ambiente físico é hostil ou em áreas que estão expostas às inclemências do tempo (leitores de acesso de portas que devem estar expostas ao vento, pó, chuva, neve, gelo e, ocasionalmente, goma de mascar, papel ou cinzas de cigarro e deve ser protegido).

Dois padrões de cartões inteligentes sem contato, o ISO/IEC 14443 e o ISO/IEC 15693 são bons candidatos para usar-se em aplicações de controle de acesso físico. Estes padrões para cartões inteligentes sem contato satisfazem os requerimentos de aplicação para maior segurança (por exemplo, técnicas biométricas ou outras técnicas avançadas de autenticação), para acomodar múltiplas aplicações em um único cartão (por exemplo, acesso físico, acesso lógico, transações de pagamento) e para proteger a privacidade da informação do portador do cartão, para implementação de novos sistemas de controle de acesso.

ISO/IEC 14443 é uma tecnologia com 13.56 MHz com um raio de ação operacional de até 4 polegadas (10 centímetros). O ISO/IEC 14446 foi originalmente desenhado para emissão eletrônica de passagens e pagamentos eletrônicos. Para estas aplicações, raios de ação operacionais curtos e velocidades de transação rápidas eram críticas. Os mesmos requerimentos de mercado levaram o ISO/IEC 14446 a ser adotado para o transporte, compras fora d elinha e transações fora de vendas. Como as aplicações usando ISO/IECV 14443 geralmente requerem um valor armazenado no cartão, o novo desenvolvimento de produtos se enfocou sobre a segurança, oferecendo-se com esta nova tecnologia uma memória central segura e esquemas sofisticados de criptografia apoiados por vários co-processadores criptográficos.

Os produtos ISO/IEC 1443 estão começando a mover-se ao mercado de controle de acesso físico. As credenciais que estão em conformidade com o ISO/IEC 14443 oferecem soluções que vão desde os cartões de memória de baixo custo até cartões com microprocessadores de alta segurança. Cartões microprocessadores oferecem níveis de interoperabilidade e segurança idênticos aos níveis oferecidos por soluções de cartões inteligentes de contato. Devido a que os cartões ISO/IEC 14443 transferem grandes blocos

de dados rapidamente, muitas das fechaduras de acesso físico habilitadas por fatores biométricos disponíveis hoje estão usando cartões ISO/IEC 14443. Vários produtos permitem taxas de transmissão de dados de até 848 kilobites/segundo, e uma emenda para modificar o padrão foi submetida às organizações de padrões para incluir essas taxas de transmissão de dado mais elevadas.

ISO/IEC 15693 é uma tecnologia de radio frequência passiva de 13.56 MHz desenhada para operar em um raio de ação de 1 metro (3 pés), enquanto ainda satisfaz os limites de saída de energia (FCC) dos EEUU. A especificação pode ser usada para o controle de acesso a estabelecimentos em edifícios onde os raios de ação de leitura podem ser estabelecidos de 4 a 6 polegadas (10 a 15 centímetros) para as portas do edifício. O ISO/IEC 15693 também é ideal para estacionamentos onde os carros e os leitores podem ser colocados para operar em raios de ação maiores, para que não seja necessário que o condutor estenda a mão para fora do carro.

A tecnologia ISO/IEC 15693 foi desenvolvida para operar em raios de ação mais amplos. As aplicações iniciais usando essa tecnologia incluíam rastreamento e etiquetagem de bens, as quais requerem maiores raios de ação operacionais e a transmissão de blocos de dados mais largos. A razão das capacidades desta tecnologia, a mesma se tornou uma das tecnologias mais preferidas para o acesso físico. Raios de ação operacionais de maior distância suportam as capacidades que os usuários esperam quando eles se acercam a uma porta. O armazenamento de leitura/escritura dos formatos biométricos, dados e informação pessoal está também levando a migração de 125 kHz a cartões inteligentes sem contato como ISO/IEC 15693.

As Tecnologias ISO-IEC 14443 e ISO/IEC 15693 evoluíram com suas próprias características e especificações. Os pontos que diferenciam as tecnologias são seus raios de ação operacionais, velocidade (“data transfer rate”), e a maturidade e a extensão das características e das aplicações que usam as tecnologias. A figura 4 sumariza as características especificações chaves que estão geralmente disponíveis para os produtos que suportam os dois padrões de cartões inteligentes sem contatos ao tempo desta publicação.

Figura 4: Características e Especificações Chaves dos Cartões Inteligentes Sem Contato

CARACTERÍSTICAS	ISO/IEC 14443	ISO/IEC 15693
Padrões	ISO/IEC 14443 ISO/IEC 7810	ISO/IEC 15693 ISO/IEC 7810
Frequência	13.56 MHz	13.56 MHz
Raio de ação operacional (ISO⁷)	Até 10 centímetros	Até 1 metro
Tipos de Chip Apoiados	Micro-controlador Lógico Fiação de Memória	Fiação Lógica de Memória
Funções⁸ de Autenticação e Criptografia	MIFARE, DES/3DES, AES, RSA ⁹ , ECC	Abastecedor Específico DES/3DES
Alcance da Capacidade de Memória	64 até 64K bites	256 e 2K bites

7 Distancias especificadas pelos padrões ISO/IEC. A implementação de acesso físico estabeleceria um raio de ação operacional específico, tipicamente até 15 centímetros (“6 inches”).

8 Os padrões ISO/IEC não especificam funções de seguridade.

9 Criptografia e autenticação de base RSA pode não estar disponível em todos os cartões devido ao consumo de energia, tempo de execução ou dificuldades do largo da chave.

Habilidade de Leitura/Escrita	Lê / escreve	Lê / escreve
Taxa de Transferência de Dados (kb/seg)	Até 106 (ISO) Até 848 (disponível)	Até 26.6
Anti-Colisão	Sim	Sim
Autenticação do Cartão ao Leitor	Desafio/Resposta	Desafio/Resposta
Capacidade do Cartão Híbrido	Sim	Sim
Suporte de Interface de Contato	Sim	Não

Tecnologias de cartões inteligentes de contato

Os cartões inteligentes de contato relacionados com o padrão ISO/IEC 7816, atualmente, são usados por uma grande variedade de aplicações, incluindo acesso físico e lógico.

Cartões inteligentes de contato são, normalmente, usados para entradas de baixo volume onde a velocidade do acesso não é uma preocupação primária, tais como áreas internas ou de alta segurança onde o uso de fatores múltiplos mitiga a vantagem que os cartões sem contato oferecem para um acesso mais rápido. Os cartões inteligentes de contato, geralmente, não são usados em sistemas de acesso físico relacionados com um alto volume de usuários e milhares de acessos diários, requer resistência ao clima e ao vandalismo, o que necessita acesso altamente conveniente ao usuário. No entanto, a tecnologia de cartão inteligente de contato é mais madura e oferece capacidades de processamento avançadas que, atualmente, não estão disponíveis em tecnologias sem contato (por exemplo, processadores mais avançados, maior capacidades de memória, sistema operativos avançados). Por esta razão, as organizações que precisam dessas características podem requerer uma aproximação aos cartões inteligentes de contato.

A escolha de qual tecnologia de cartão inteligente é apropriada para um novo sistema de acesso físico seguro deveria ser determinada pelas necessidades organizacionais de curto e longo prazo. Ao identificar os requerimentos imediatos e futuros do sistema, as organizações podem selecionar as tecnologias que melhor satisfaçam as metas gerais de implementação.

Requerimentos e Problemas de Interface do Usuário

Volumem de Passo e facilidade de uso são considerações chaves num sistema de segurança física. Numa instalação grande, milhares de empregados precisam obter acesso num curto período de tempo. A tecnologia sem contato tem vantagens definitivas de volume de passo sobre a tecnologia de contato ou de inspeção visual de crachás. No entanto, certas compensações devem ser tomadas em conta.

A Facilidade de Uso Vs. Desempenho e Segurança

Qualquer decisão relacionada com um sistema de controle de acesso e a escolha de uma credencial de identificação devem equilibrar-se com a

facilidade de uso para o portador do cartão, com o desempenho e a segurança do sistema e da identificação. Uma avaliação cuidadosa destes e outros requerimentos organizacionais é o primeiro passo para selecionar uma tecnologia sem contato ou de contato.

O ambiente sem contato tem óbvias vantagens em termos de velocidade e de facilidade de uso. Os problemas ocasionados pela necessidade de alinhar o cartão ao leitor ou a inserção de um cartão num leitor são eliminados, por tanto aumenta o volume de passo (a menos que se tenha um requerimento de autenticação com múltiplos fatores, tais como, um PIN ou biométrie). No entanto, em alguns casos um ambiente de contato pode ser considerado um sistema mais seguro se existirem preocupações de que as sinais de radio-freqüência dos cartões sem contatos estejam sendo comprometidos (já que a conexão física entre o cartão e os leitores reduz o potencial de comprometimento de sinais sem fio). Usando as senhas e contra-senhas, e outras técnicas criptográficas na implementação de cartões inteligentes sem contato ajudam a minimizar este risco.

O raio de ação operacional das tecnologias sem contato é uma consideração importante para a facilidade de uso. Os raios de operação mais longos podem ser a solução preferida quando o volume de passo através do ponto de acesso e a conveniência do usuário são as principais considerações, ou quando se requer acesso “de mãos livres”. Um raio de operação menor pode ser preferido quando outros fatores de autenticação são requeridos.

Qualquer decisão de implementação deve tomar em conta a compatibilidade com as políticas gerais e procedimentos de segurança física.

Impacto do “Americans with Disabilities Act” (Lei para Pessoas com Impedimentos).

Instalações públicas nos Estados Unidos, atualmente, requerem o comprimento dos regulamentos impostos pelo “Americans with Disabilities Act”. Este requerimento pode influenciar a seleção de uma tecnologia de segurança apropriada, já que as organizações devem considerar questões como destreza manual e outras limitações físicas. Para usuários que podem estar confinados à cadeira de rodas ou que precisam assistência para mover-se, o requerimento sobre a orientação do cartão dentro do leitor pode ser um problema. Ainda mais, pode haver problemas com a apresentação do cartão perto do leitor (distância cartão-leitor). Pode ser necessário instalar os leitores mais perto do chão para o acesso com cadeiras de roda. Um raio de ação operacional maior oferece vantagens para usuários com impedimentos.

Considerações no Nível de Sistema

A seleção de um desenho de sistema e arquitetura de segurança deve ser determinada pelos requerimentos de desempenho e interface com o usuário, assim como requerimentos para a integração com outros sistemas de segurança ou não relacionados com segurança (como recursos humanos e controle de edifícios). Adicionalmente, o funcionamento dos vários componentes do sistema (credencial, leitor, painel, servidor de controle de acesso, base de dados) deve ser examinado para assegurar que o sistema está desenhado com a segurança, flexibilidade e a capacidade de escalamento (“scalability”) desejada.

Sistemas Centralizados vs. Distribuídos

Uma consideração básica num desenho de um sistema é se o sistema deve ser centralizado ou distribuído. Essa decisão determina boa parte do funcionamento do sistema. Devem tomar-se decisões como, onde armazenar os PINS ou os padrões biométricos e, em que nível de criptografia deve ser incluído numa credencial. Armazenagem central versus armazenagem no cartão têm diferentes implicações para a vulnerabilidade dos dados devido a diferentes tipos de ameaça e para a proteção de informação privada.

Sistemas Abertos versus Sistemas Proprietários.

Outro fator no desenvolvimento de um sistema de acesso físico seguro é o grau em que é desejável a integração com outros sistemas de segurança (na próxima seção se discute interoperabilidade em maior detalhe). Estes outros sistemas podem incluir dispositivos para detecção de intrusos, câmaras de vigilância, armazenagem de vídeo e controles de edifício. Quando se requer soluções inter-operativas, o sistema deve ser desenhado para incorporar uma arquitetura aberta e interfaces programáticas de aplicação padrão (APIs) na medida do possível.

De fato, a melhor abordagem para definir os requerimentos para um sistema de acesso físico seguro é adotar uma visão de segurança em toda a empresa. Ao tomarem-se decisões sobre soluções e tecnologias de segurança individual ao mesmo tempo em que vão sendo encaixadas num plano holístico de segurança no nível de toda a empresa, se podem tomar decisões que pagam dividendos de longo prazo e eliminam medidas temporárias que podem resultar da implementação de sistemas isolados e fechados.

A tecnologia a ser usada deve ser escolhida cuidadosamente. Selecionando um sistema com base numa arquitetura aberta usando APIs abertos tem certas vantagens, como integração mais fácil com outros sistemas, flexibilidade para compras, maior facilidade de expansão e capacidade de escalamento ("scalability"). Numa análise final, sistemas proprietários ou fechados podem ter uma vantagem de custo ou de tempo de implementação em curto prazo, mas em longo prazo sacrificam flexibilidade, capacidade de escalamento ("scalability") e integração.

Interoperabilidade

A interoperabilidade é um elemento chave no desenho e implementação de uma solução para o controle do acesso físico. O significado de interoperabilidade é, freqüentemente, entendido diferentemente em vários negócios e organizações. No entanto, alguns pontos importantes a considerar são os seguinte:

- Como as novas tecnologias interagem com os sistemas de acesso físico ou lógico preexistentes?.
- Como interagem entre si produtos sem contato disponíveis a vários vendedores?.
- Como afeta os sistemas de acesso físico e lógico a infra-estrutura da empresa e outras aplicações?.

A interoperabilidade deve ser considerada no contexto de várias opções disponíveis para solucionar o controle do acesso físico.

A tecnologia de velocidade de 125 kHz é amplamente usada e será tipicamente o sistema preexistente que está sendo atualizado ou que deve ser integrado com um novo sistema. Um dos grandes problemas com os sistemas de proximidade de 125 kHz é que não estão ligados a nenhum padrão oficial, mas são soluções proprietárias do vendedor ou, na melhor das hipóteses, sujeitas a padrões. Esse problema é de particular importância quando uma organização está implementando ou integrando uma nova tecnologia de cartões inteligentes. Poderá ser (por exemplo) necessário planejar a implementação de múltiplas tecnologias sem contato até que se complete a migração da infra-estrutura da empresa as tecnologias de cartões inteligentes sem contato mais novas.

Os padrões de cartões inteligentes – ISO/IEC 7816, ISO/IEC 14443 e ISO/IEC 15693 – especificam como os componentes interagem até certo nível, na qual diferentes padrões respaldam funções inter-operativas a diferentes níveis. Os padrões não incluem todos os componentes ou características de segurança necessárias para respaldar a implementação completa do sistema. Os cartões inteligentes que incluem microprocessadores oferecem mais flexibilidade para implementar protocolos interoperativos. Ademais, a introdução do sistema operativo de cartões de propósito geral (general purpose) cria uma plataforma genérica que pode ser usada por várias aplicações.

Solução do Cartão vs. Solução do Leitor. Exigir que cartões e leitores estejam em conformidade com um único padrão ISO/IEC não é suficiente para assegurar a interoperabilidade entre sistemas e dispositivos de diferentes fabricantes, provedores de aplicações ou integradores. A certo nível, a interoperabilidade pode ser conseguida, usando um leitor interoperativo ou um cartão interoperativo. Cada abordagem implica diferentes custos e tem diferentes vantagens e desvantagens.

Muitos fabricantes de leitores estão, agora, oferecendo leitores que podem ler e escrever em cartões que cumprem com os padrões ISO/IEC 14443 e ISO/IEC 15693. Outros produtos estão disponíveis e podem comunicar-se tanto com cartões que satisfazem o ISO/IEC 14443 e o ISO/IEC 15693, usando um único micro-circuito (chip) leitor.

Quando se escolhe a tecnologia de cartões inteligentes de contato ou sem contato, os programadores de sistemas devem revisar em que nível é apoiada a interoperabilidade e como os produtos se acomodam às funções no mesmo padrão.

Para resolver o problema da falta de interoperabilidade em segurança e em padrões de aplicação, as organizações usuárias podem colaborar para desenvolver especificações para interoperabilidade com padrões da indústria. Por exemplo:

- A especificação EMV foi desenvolvida pela indústria financeira para cartões inteligentes de contato usados para aplicações de pagamento de crédito e de débito.
- A especificação da interoperabilidade de cartões inteligentes do governo (GSC-IS) oferece soluções a uma gama de questões de interoperabilidade associadas com a implementação de tecnologia de cartões inteligentes de contato. Permite ao programador da aplicação desenvolver aplicações para o cliente sem ter um conhecimento íntimo das interfaces do cartão. A especificação se fez para oferecer a habilidade para desenvolver cartões inteligentes de identificação

seguros que podem operar em múltiplas agências de governo ou entre governos federais, estaduais e locais. Uma próxima revisão do GSC-IS, administrado pelo “National Institute of Standards and Technology” (NIST), incluirá definições da interoperabilidade para tecnologias de cartões inteligentes sem contato oferecendo um recurso para a indústria que pode ser usado para a implementação de cartões inteligentes sem contato.

Administração do Ciclo de Vida

Uma questão crítica para a implementação de um sistema de acesso físico é a necessidade de rastrear cada cartão de acesso e cada aplicação no cartão. Uma função singular de um cartão inteligente é a sua capacidade de armazenar ou modificar aplicações depois que o cartão foi emitido (também chamado personalização pós emissão). Devido a que a informação num cartão inteligente pode ser modificada em forma dinâmica, é necessário rastrear o ciclo de vida das aplicações de um cartão e do ciclo de vida de um cartão. A administração do ciclo de vida¹⁰ rastreia e, em alguns casos, administra todas as mudanças aos dados do cartão inteligente, independentemente de que a informação no cartão seja uma nova versão de uma aplicação, uma nova tecnologia de chip, ou uma informação atualizada sobre o portador do cartão.

No nível mais simples, a administração do ciclo de vida pode ser concebida como uma base de dados vinculada a uma aplicação específica de controle de acesso. A base de dados registra informações sobre o estado das transições e dos dados do ciclo de vida, como as seguintes:

- O tipo de cartão, como um cartão de empregado, contratante ou visitante.
- Informação sobre pedidos e autorizações de cartões.
- Informação sobre personalização do cartão, incluindo:
 - A versão do sistema operativo e os dados do chip
 - Dados de personalização, incluindo elementos visíveis como uma foto, assinatura ou código de barras.
 - Vínculos da base de dados.
- Informação sobre a administração da aplicação, incluindo:
 - O estado dos privilégios (emitidos ou atualizados).
 - Informação sobre expiração, substituição ou re-emissão do cartão.
 - Ativação, suspensão ou reativação da aplicação (bloqueio e desbloqueio reversível).
 - Pós-emissão de aplicações.

O inventário dos cartões de controle de acesso deve ser rastreado e feito auditoria para proteger contra a emissão de cartões não autorizados. A administração do inventario de cartões incluem a contagem de todos os cartões recebidos e distribuídos aos centros de emissão. Portanto, o ciclo de vida do cartão começa com um registro do número de série do chip dado pelo fornecedor do cartão. A administração do ciclo de vida, subseqüentemente rastreia todas as adiçõs ou modificações feitas aos dados que estão armazenados em cada cartão individual, e simplifica o

¹⁰ Os seguintes documentos do “Global Platform” e do “Open Security Exchange” oferecem uma revisão mais completa do tema de administração do ciclo de vida do cartão: “A Primer to the Implementation for Smart Card Management and Related Systems,” disponível no www.globalplatform.org; “Physical Security Bridge to IT Security,” disponível no www.opensecurityexchange.com

processo de re-emissão do cartão, assegurando que o novo cartão tenha o mesmo conjunto de aplicações e valores de parâmetros de aplicação incluídos no cartão original.

Cartões de Acesso de Aplicação Única

Cartões de controle de acesso de aplicação única vinculam uma aplicação a um cartão. Para tais cartões, a aplicação e o cartão são administrados como um ciclo de vida. Para muitos sistemas de controle de acesso, os administradores podem controlar modificações à aplicação, solicitando aos portadores do cartão para que tragam seus cartões a uma localização específica para serem atualizados, eliminando a necessidade de substituir cartões quando se modificam privilégios ou aplicações. Neste caso, a aplicação administra qualquer modificação ao cartão, e a base de dados é atualizada.

A administração do cartão pode ser automatizada, vinculando-se a base de dados do portador do cartão à aplicação de acesso, e aplicando regras de decisão sobre privilégios de acesso. Neste caso, um sistema de administração da aplicação assegura que a informação é consistente entre as bases de dados, fornecendo uma trilha de auditoria completa que rastreia a emissão, as atualizações e a expiração ou arevocatória.

Organizações com múltiplas localizações podem usar um sistema automatizado de gestão da aplicação, para assegurar a integridade dos dados da aplicação e melhorar a segurança do sistema, assegurando, por exemplo, que o cartão emitido numa localização é válido em todas as localizações, ou que uma modificação no estado da aplicação num estabelecimento é imediatamente implementada em todas as localizações. O nível de segurança para controlar as atualizações aos dados do cartão ou à base de dados, neste caso, é controlado pela aplicação.

Cartões de Aplicação Múltipla

A tecnologia de cartões inteligentes oferece a oportunidade de incluir múltiplas aplicações em um cartão (para exemplos, ver uma próxima seção, *Novas Aplicações Habilitadas por Sistemas de Cartões Inteligentes*, na página 35). Cada aplicação pode ser administrada por um grupo diferente dentro de uma organização, ou até por um fornecedor externo de aplicações (por exemplo, uma bolsa eletrônica de terceiros para uso numa lanchonete). Ainda que a implementação de múltiplas aplicações requiera uma coordenação organizacional mais complexa, esta pode fortalecer a adoção de cartões inteligentes. A tecnologia de cartões inteligentes permite o uso de ferramentas com base na rede “web”, que permite aos usuários adicionar, modificar ou eliminar aplicações de forma segura, obviando a necessidade de que um administrador faça tais mudanças. Nestes casos, a administração do ciclo de vida deve controlar e rastrear o estado de cada aplicação armazenada no cada cartão.

A administração do ciclo de vida de uma aplicação é fundamentalmente diferente da administração do ciclo de vida de um cartão. A área funcional que emite o cartão (por exemplo, o departamento de manutenção de bens) pode estar completamente separada da área funcional que administra uma aplicação (por exemplo, informática ou recursos humanos). A administração centralizada do ciclo de vida de um cartão requer que a entidade que o emite seja responsável pela produção inicial do cartão, e de prover uma

interfase aos outros fornecedores de aplicações para o carregamento, a personalização, e as atualizações das aplicações.

Uma vez que os cartões são emitidos, fazer mudanças aos dados ou a uma aplicação podem ser feitas desde um ponto central ou remoto, usando comunicações seguras. Um ambiente híbrido oferece a maior flexibilidade, combinando os melhores elementos, tanto de uma administração centralizada como distribuída. Quando se usa a internet para personalização pós-emissão, se requer um controle adequado para verificar a autenticidade do portador do cartão e assegurar a integridade e a criptografia dos dados. Isso requer um carregador seguro da aplicação que está baixo o controle do fornecedor da aplicação.

Ao considerar-se múltiplas aplicações para um cartão de acesso, um sistema de administração do ciclo de vida de um cartão, com base num conjunto de regras de negócio, pode manejar vários tipos de cartões e de aplicações. Este sistema pode proporcionar as seguintes funções:

- Administração centralizada da emissão de cartões, com uma interfase para cada aplicação, e para o carregamento e a personalização da aplicação.
- Administração centralizada de cartões e aplicações, aplicando regras de decisão e autorização para adicionar, modificar, bloquear e desbloquear aplicações e funções administrativas.
- Implementação de modificações a uma aplicação com base em eventos, tais como bloquear privilégios para um cartão perdido ou bloquear uma aplicação se o uso do cartão for suspeito.
- Um processo para atender solicitações de usuários para adicionar aplicações e adicionar ou modificar privilégios, e para personalizar cartões de forma segura depois de que foram emitidos.
- Uma trilha de auditoria centralizada das transições do estado de ciclo de vida das aplicações.
- Apoio e acesso do usuário aos dados sobre o estado do ciclo de vida.

Outras Considerações

A geração e a gestão de chaves são funções críticas. A geração de chaves combinadas e dos certificados digitais associados deve ser controlada durante os processos de emissão e atualização. Os esquemas de segurança devem proteger as sessões mais importantes, começando com o uso das chaves de transporte do fabricante do cartão, durante todas as modificações do ciclo de vida do cartão. O processo de preparação inicial dos dados (preparação dos conjuntos de dados únicos, “scripts” e chaves) continua sendo uma função do fornecedor da aplicação. O emissor logo oferece a infra-estrutura que permite aos cartões de identificação inteligente estar protegidos para o futuro (“future-proofed”), assegurando que as aplicações e as novas funções possam ser implementadas de forma segura depois que o cartão for emitido.

Custos e Benefícios

É um desafio quantificar com precisão os benefícios potenciais de um sistema de segurança. As iniciativas de segurança são parte de uma estratégia geral de redução de risco e os custos de mitigação devem ser comparados contra os riscos. Quando for possível, o sistema deve ser desenhado para beneficiar tanto a segurança como as operações. Por exemplo, uma credencial segura pode aumentar a segurança e o volume

de passo. Ademais, se a credencial é usada para múltiplos propósitos, os custos administrativos podem ser reduzidos.

Uma consideração muito importante no desenho e implementação de qualquer solução de negócios é determinar quem paga pelo sistema. Um sistema de segurança física pode ser visto como uma responsabilidade do departamento de segurança. Entretanto, se um sistema é considerado como outro sistema de informática, ele poderia ser considerado como uma parte da rede de informática. Ademais, como a segurança é uma função de toda a organização, pode haver muitos donos do sistema, incluindo segurança, administração de edifícios, recursos humanos ou gerência executiva.

A habilidade dos cartões inteligentes de apoiar múltiplas aplicações podem ajudar a incentivar a implementação de um novo sistema. Múltiplas organizações ou departamentos podem implementar aplicações ou compartilhar o custo do novo cartão de identificação inteligente e a sua infra-estrutura. Uma vez que a infra-estrutura do sistema de controle de acesso com base em cartões inteligentes estiver operando, o custo incrementado de adicionar novas aplicações ou funções será menor.

Compartir a carga de planificação, desenho e pagamento de um sistema de segurança física permite que se tomem decisões que resultaram numa solução flexível e ampliável de segurança física. O processo deve incluir a avaliação do requisito de arquitetura aberta com a meta de alcançar um sistema integrado que operará múltiplas aplicações.

Tendências de Mercado

Ambos, o governo e a indústria estão atualmente juntos na implementação de aplicações basadas na tecnologia de cartões inteligentes. Muitas destas aplicações usam os cartões inteligentes para acesso a prédios e a outras facilidades. As aplicações em outros mercados verticais, como as instituições financeiras e o comércio, têm o potencial para obter um acesso físico por meio de cartões no futuro. Para proporcionar cenários de múltiplas aplicações, os desenvolvedores da tecnologia estão introduzindo cartões com variedades de tipos de relação com contatos e sem contatos.

Governo

Nos Estados Unidos, o governo federal está dando apoio para o uso de tecnologia de cartões inteligentes para milhões de cartões de identificação de empregados federais.

- A Administração de Serviços Gerais ou “General Service Administration” (GSA) desenvolveu uma especificação para cartões inteligentes de aplicação múltipla (GSC-IS), e várias agências estão planejando usar cartões que cumpram com esta especificação para o acesso físico.
- O Departamento de Estado ou “Department of State” (DoS) está implementando um sistema de controle de acesso para os seus estabelecimentos em Washington DC. Os cartões inteligentes de contato serão emitidos a empregados do DoS e contratantes para o acesso físico e lógico.
- O Departamento de Defesa ou “Department of Defense” (DoD) está emitindo credenciais de cartões inteligentes a milhões de pessoas, entre elas, militares, empregados civis e contratantes como parte do programa Cartão de Acesso Comum ou “Common Access Card” (CAC). Estes

cartões oferecem, atualmente, uma plataforma comum para PKI, acesso lógico e identificação que cumprem com os requerimentos da Convenção de Genebra, e forneceram acesso físico no futuro.

- A Administração de Segurança do Transporte ou “Transportation Security Administration” (TSA) está testando diferentes tecnologias de acesso físico e lógico dentro do programa Credencial de Identificação do Trabalhador do Transporte ou “Transportation Worker Identification Credential” (TWIC). Este programa poderá estender-se a trabalhadores de transporte do setor público e privado no nível de todo o país.

Muitas agências de trânsito que têm introduzido tecnologia de cartão inteligente sem contato para o pago de passagens estão agora explorando o uso da mesma tecnologia para o acesso as instalações e equipamento. A autoridade de transporte da área metropolitana de Washington ou “Washington Metropolitan Area Transit Authority” (WMATA) está usando a tecnologia de cartão de passagens SmarTrip™ para o acesso dos empregados aos escritórios da WMATA. Ademais, a WMATA e o Departamento de Educação ou “Department of Education” (DoE) apresentaram um cartão inteligente sem contato para as credenciais de empregados da DoE que é utilizado para o acesso às instalações e para o pagamento das passagens de transporte. A autoridade de transporte de Chicago introduziu tecnologia de cartão inteligente sem contato para o pagamento de passagens e têm usado cartões de proximidade para o acesso às instalações e ao equipamento, tais como as gavetas de dinheiro nos ônibus.

Uma revisão da especificação do cartão inteligente GSA que inclui a tecnologia de cartão inteligente sem contato será emitido no verão de 2003. Demonstrações da tecnologia sem contato para acesso físico são planejadas pelos Departamentos de Interior e de Tesouro. Os cartões de tecnologia sem contato podem ser considerados para o uso nas portas e em outras instalações de transporte, onde a rápida movimentação é essencial.

Comercial

As indústrias comerciais estão utilizando aplicações de tecnologias de cartão inteligente. Numerosas corporações de comércio, incluindo Sun Microsystems, Microsoft, Schlumberger, Shell, Boeing e Proctor & Gamble¹¹ têm implementado ou estão planejando implementar cartões de identificação inteligente para o acesso físico e lógico.

Os cartões inteligentes estão sendo usados para pagamentos ao redor do mundo, com as iniciativas atuais da American Express, JCB, Máster Card e Visa International para estender o uso de cartões inteligentes para o pagamento sem contato. Por exemplo, em Orlando, Florida, a Master Card e vários bancos emitiram milhares de cartões inteligentes sem contato no projeto piloto Master Card PayPass. Neste projeto piloto, os cartões inteligentes sem contato foram usados em praças de alimentação e lojas, onde a velocidade das transações e a conveniência dos clientes são consideradas os maiores benefícios.

Ao tempo em que a tecnologia sem contato cresce em varias indústrias, o potencial aumenta para os cartões de múltipla aplicação, que poderiam ser usados para identificação, acesso físico, pagamento, e para outros propósitos. Atualmente, muitos governos estrangeiros estão emitindo estes

¹¹ “Building Blocks of the U.S. Smart Card Market,” *Card Technology*, May 2003.
Smart Card Alliance © 2003

tipos de cartões de múltipla aplicação. Em alguns lugares, como Hong Kong, o uso de tecnologia sem contato para o pago de passagens de transporte público está sendo expandido para suportar formas adicionais de pagamento e outras funções. A tecnologia que pode suportar esses programas já existe. Os desafios estão em juntar os programas dos setores público e privado, e resolver problemas da administração de programa, custos de fusão e privacidade.

Tecnologias emergentes

Novos produtos estão sendo lançados, os quais facilitarão o uso de tecnologia de cartão inteligente sem contato para o controle de acesso físico. Os sistemas de controle de acesso físico estão sendo empregados para aceitar cartões de registro ISO/IEC 14443 que são reconhecidos com apenas passar o cartão levemente num leitor de cartões de registro ISO/IEC 15693 com um raio de ação operacional expandido ou cartões inteligentes de contato que são introduzidos em um leitor.

As organizações têm um número de opções de tecnologia de cartão de identidade inteligente, incluindo cartões de tecnologia múltipla, cartões híbridos e cartões de interfase dupla. Para que pessoas de diferentes organizações tenham acesso às instalações, sistemas de controles de acesso estão sendo desenvolvidos com cartões e leitores de cartões que podem suportar múltiplas tecnologias de identidade. Por exemplo, um cartão inteligente de contato ou sem contato pode incluir tecnologia legada como as fitas magnéticas ou os códigos de barra. Os cartões de tecnologia múltipla disponíveis podem combinar as tecnologias sem contato de padrão ISO/IEC com tecnologia de proximidade de 125 kHz, permitindo aos cartões funcionar com sistemas de acesso físico legado e como os novos sistemas de registros ISO/IEC.

Cartões de interfase dupla estão sendo introduzidos para incorporar ambas as interfases, de contato e sem contato, em um único cartão com um chip. Cartões inteligentes híbridos com dois chips estão disponíveis (um com contato em um sem contato). Esses produtos permitem as organizações combinarem aplicações de acesso físico sem contato com as aplicações que requerem uma interfase de contato, como o acesso lógico aos computadores e as redes. Esta integração de acesso físico y lógico pode gerar enormes benefícios de seguridade. Organizações podem juntar os privilégios do acesso físico e lógico para aumentar a seguridade (por exemplo, o requerimento de usar o cartão para deixar uma instalação pode reduzir o acesso não autorizado aos computadores dos empregados e melhorar a reposta de emergência se houver uma catástrofe na instalação). Este tipo de integração programática pode reduzir a emissão do cartão e os custos de administração, e oferecer aos usuários a conveniência de uma única credencial de identidade de acesso.

Para oferecer fatores adicionais de autenticação, os cartões inteligentes podem incluir múltiplos dados biométricos. Os formatos biométricos podem ser guardados no cartão o em outros componentes do sistema de controle de acesso.

Os novos sistemas de controle de acesso físico com bases em cartões inteligentes podem prover as organizações com maiores flexibilidades. Tais sistemas incluem componentes programáveis, permitindo privilégios de acesso serem modificados em pleno trabalho para atingir as condições de ameaça e os requerimentos necessários. Ademais, os componentes com

base em TCP/IP estão prontos para a rede, permitindo a monitorização centralizada das instalações em diferentes localidades.

Migração ao Sistema de Identidade de Acesso Físico com Base em Cartões Inteligentes

Uma organização pode mudar-se para um sistema de identidade de acesso físico com base em cartão inteligente por muitas razões, por exemplo, para melhorar a segurança, implementar processos de identificação mais eficientes, reduzir número de cartões de identidade usados, oferecer acesso a novos lugares ou agregar novas aplicações. Indiferentemente das razões, a implementação desses sistemas requer considerações sobre se o novo sistema substituirá sistemas velhos ou se ele precisa ser integrado e é compatível com os sistemas legados. Enquanto a solução ideal pode substituir todos os sistemas velhos imediatamente, mover-se a um novo sistema com base em cartão inteligente pode precisar ser realizado de forma incremental (o que requer um plano para fazer o movimento com a menor quantidade de custos e desorganização). Tal plano, chamado um “plano de migração”, deve considerar todos os componentes do sistema de controle de acesso físico e deve desenvolver uma estratégia que acolha os novos requerimentos, ao mesmo tempo em que impulsa os investimentos existentes e gerência a experiência do portador da credencial durante o processo de migração.

Algumas questões-chaves que devem ser consideradas no planejamento da migração incluem:

- Qual é o tempo desejado para substituir sistemas legados? Quantos sistemas legados estão em execução? Estão diferentes legados em execução em diferentes lugares? Há novos lugares que devem ser considerados?
- Quais pontos de acesso requerem novos leitores? Requerem todos os pontos de acesso, ou alguns de, novas funcionalidades (exemplo, dados biométricos ou teclas de PIN) ou se requer nova funcionalidade somente em sítios selecionados? Quais tecnologias de identificação são requeridas para acolher os requerimentos de segurança nos pontos de acesso?
- Quais empregados requerem de novas funcionalidades nos cartões de identidade? É desejável substituir todos os cartões de identificação para melhorar a segurança e adicionar funcionalidade através da organização ou são os cartões de identificação, somente, necessários para um grupo de empregados?
- Mudarão os formatos de dados ou os esquemas de numeração dos sistemas de identificação? Como serão modificados os sistemas legados para acomodar essas mudanças?
- Há novos requerimentos de segurança que exigirão modificações ou melhoramentos na arquitetura do sistema de acesso físico ou nos seus componentes?

Considerações-chaves de migração

Algumas das decisões-chaves de migração referem-se a quais novas tecnologias de cartão e de leitor são escolhidas e a como o sistema maneja formatos de dados legados.

Cartões de tecnologia múltipla

Os cartões de identificação podem ser compostos de muitos elementos diferentes, cada um específico para uma circunstancia particular, como:

- Foto impressa do portador do cartão
- Nome impresso do portador do cartão
- Código(s) de barra (s)
- Fita magnética
- Fita de débito
- Tecnologias sem contato múltiplas (125 kHz, 13.56 Mhz)
- Tecnologia de cartão inteligente de contato
- Fita ótica
- Relevô
- Marcação de seguridade¹²
- Painel de assinatura
- Emissão do endereço e logo tipo da autoridade

O uso de cartões de tecnologia múltipla podem ser parte de uma estratégia de migração o a mesma solução. Ao considerar-se um cartão de identificação inteligente de tecnologia múltipla, é importante lembrar que a combinação de um pequeno número de tecnologias compatíveis de identificação podem ser uma solução prática, em quanto outras combinações podem ser impossíveis ou não práticas de implementar-se.

Cartões de tecnologia múltipla oferecem uma solução potencial sempre que as novas tecnologias e as legadas possam co-habitar. Por exemplo, um chip de proximidade legado de 125 kHz pode co-habitar com um novo chip de cartão inteligente sem contato de 13.56 MHz, e as tecnologias não interferirão umas com as outras. Cartões de tecnologia múltipla de 125 kHz e de 13.56 MHz estão atualmente disponíveis. De igual forma, tecnologia de cartão inteligente de contato pode co-habitar com tecnologias sem contato de 125 kHz e 13.56 MHz.

Tecnologias sem contato (125 kHz e 13.56 MHz) e de cartões inteligentes com contato podem trabalhar com outras tecnologias de identidade como as fitas magnéticas, os códigos de barra e as fitas óticas. Tal cartão de tecnologia múltipla pode oferecer ao usuário uma credencial de cartão de identificação única que é compatível com sistema instalados, ao tempo em que se disponibilizam tecnologias mais novas.

Quando é tecnicamente possível misturar varias tecnologias em um cartão, há de ser cuidadoso ao considerar-se o impacto geral. As restrições do cartão de tecnologia múltipla são:

- **Inclusão de tecnologias múltiplas sem contato que operam a mesma freqüência.** Em geral, os cartões não podem incluir tecnologias múltiplas sem contato (125 kHz e 13.56 MHz) que operam a mesma freqüência uma vez que interferirão umas com as outras.
- **Espessura do cartão.** O padrão ISO/IEC 78 dias define a espessura máxima permitida para um cartão. Cartões de tecnologia múltipla cumprem com estas especificação máxima de espessura. De outra maneira, os leitores de contato que requerem que os cartões sejam de

12 Marcação de seguridade pode ser usada para DETER TAMPERING AND COUNTERFEITING. Tecnologias como os marcos ornamentais, microtexto, texto ultravioleta, hologramas, KINEGRAMAS, imagens de lazer múltiplo e lazer são alguns exemplos. Ademais dos custos de impressão, a marcação de seguridade pode ser necessária se TAMPERING AND COUNTERFEITING se são uma ameaça real ou percebida.

Smart Card Alliance © 2003

-
- certa espessura máximo podem não ser capaz de ler o cartão.
 - **Lugar de relevo.** Se um relevo é necessário, o local do chip, a espiral da antena, o cabo Wiegand ou o local do dado ótico deve ser considerado de forma que essas áreas não sejam afetadas pelo processo de relevo.
 - **Custo do cartão.** Em teoria as companhias podem desenhar cartões que suportem qualquer combinação de tecnologia de identificação e sem contato. Na pratica, no entanto, a complexidade e o custo desse cartão pode limitar sua aceitação no mercado. Complexos cartões de tecnologia múltipla tem custos invariáveis mais que a soma das suas pecas.
 - **Capacidade de manufatura e disponibilidade de cartões.** Cartões de tecnologia múltipla sem padrão podem ser feitos, mas pode haver um maior tempo para engenhar a estrutura do cartão e para qualificar os processo de produção em concordância com os procedimentos ISO. Se múltiplos produtores estão envolvidos em fornecer as diferentes tecnologia, os problemas de garantia podem ser uma preocupação.
 - **Taxa de falhos do cartão.** Cada tecnologia tem o potencial para introduzir possíveis falhas (funcional o estética) durante a produção do cartão, aumentando o risco deter que desfazer-se do cartão. Ademais, quanto maior o número de tecnologias agregadas ao cartão maior o risco do mesmo de apresentar uma taxa de falhos mais alta uma vez emitidos. Períodos de vida mais curtos afetam o custo total, o qual não só inclui o custo da substituição de um cartão, mas também os custos operacionais de re-emissão.

A combinação de um pequeno número de tecnologias de identificação compatíveis em um cartão único é mais fácil e pode ter maior custo - beneficio que a combinação de varias tecnologias. Em quanto os cartões de tecnologia múltipla podem oferecer soluções para a acomodação de sistemas de controle de acesso legado, organizações devem considerar a complexidade agregada da implementação e manutenção de tecnologias múltiplas.

Cartões de Aplicação Múltipla

As organizações podem preferir usar uma única tecnologia de cartão inteligente que pode suportar tanto o sistema legado como novas aplicações. Um cartão inteligente de aplicação múltipla pode permitir cada dado de tecnologia de aplicação legado ser armazenado na sua própria área com suas chaves secretas. Por exemplo, um chip de cartão de identificação inteligente sem contato pode comunicar com um leitor usando 13.56 kHz, mas usa os formatos e os dados requeridos por um sistema de controle de acesso legado de 125 kHz. Um cartão inteligente único de contato ou sem contato pode ser altamente desejável a razão do custo reduzido e de uma maior conveniência.

Leitores de Tecnologia Múltipla

O uso de um leitor de tecnologia múltipla é outra abordagem à migração. Leitores de tecnologia múltipla podem ler mais de uma tecnologia ao mesmo tempo. O leitor pode ser simples ou complexo, dependendo se as tecnologias podem coabitar. O protocolo e a interfase física do leitor ao painel é tipicamente a mesma para ambas as tecnologias, mas o conteúdo não. Um leitor de tecnologia múltipla pode, então, ser tão simples como dois leitores separados em uma caixa, cada um com seu próprio fluxo de saída de dados; ou pode ser um leitor mais sofisticado que leia mais de uma

tecnologia e transmita os dados do cartão usando uma única interfase e cabos.

Sistemas de controles de acesso físico que usam tecnologias RF múltiplas operando na mesma freqüência pode ser combinado com custo benefício em um único cartão; por exemplo, chips de leitura e leitores de tecnologia múltipla estão atualmente disponíveis em formatos que suportam ISO/IEC 14443 e ISO/IEC 15693.

Fiação do Sistema de Controle de Acesso

O custo de migração de um componente que é, frequentemente, desatendido, é a requisição de nova fiação ou a substituição da mesma. Muitos sistemas de controle de acesso atuais usam tecnologia de leitura única que requer somente alguns fios entre o leitor e o painel. Se novas funções de controle de acesso requerem um protocolo de comunicação de duas vias (por exemplo, RS-232, RS-485 ou TCP/IP) entre o leitor e o painel, um tipo diferente de fiação pode ser necessário (por exemplo, fiação de categoria 5 ou similar). Puxar novos fios através de um edifício pode ser caro e, em alguns casos, impossível sem maiores modificações ao mesmo edifício.

Formatos dos Dados de Controle de Acesso

Ao mover dados da velha tecnologia de um cartão de identificação de acesso físico ao novo cartão com base em chip pode ser uma consideração chave, dependendo em quantos cartões estão envolvidos e se os portadores de cartão estão distribuídos geograficamente. Uma aproximação ao movimento de dados é a duplicação dos mesmos de um cartão de 125 kHz a um cartão inteligente. Esta solução é particularmente atrativa porque leitores de cartão inteligente estão disponíveis com a mesma interfase de saída como os leitores de 125 kHz, assim que os painéis de controles de sistema de acesso não precisariam ser substituídos.

Novos sistemas de acesso físico podem ter novos dados ou novos formatos de dados que são incompatíveis com os sistemas legados mais antigos. Isto requererá uma estratégia de migração que emite novos cartões e incorpora novos leitores, painéis e funcionalidades de servidores de controle de acesso que pode entender o novo formato, mas isso também considera como os formatos legados podem ser apoiados durante a migração.

Conclusão

É crítico para uma organização definir os objetivos a longo prazo para um novo sistema de identificação de acesso físico, desenvolver uma estratégia de migração cuidadosa e um plano que implemente o sistema de forma lógica, conveniente e com benefícios de custo e tempo. Migrar a uma nova tecnologia de controle de acesso pode ser econômica e relativamente sem rodeios se a mudança é bem planejada.

Aplicações Permitidas Pelos Sistemas De Cartão Inteligente

O uso de cartões inteligentes permite a um sistema de controle de acesso incluir aplicações que fazem mais que autorizar o acesso físico. Tomando vantagem das capacidades do chip do cartão inteligente, as organizações podem melhorar os meios para implementar um novo sistema de controle de acesso físico e aumentar a habilidade desse sistema de controlar necessidades futuras.

Esta seção descreve três aplicações que são regularmente implementadas junto com o controle de acesso físico dos cartões inteligentes de aplicação múltipla:

- Aplicações de controle de acesso lógico (por exemplo, para autenticação de computadores ou de rede);
- Aplicações de pagamento;
- Aplicações de armazenamento de dados seguros;

Aplicações de Controle de Acesso Lógico¹³

O requerimento para uma maior seguridade virtual (por exemplo, acesso seguro aos recursos de rede TI) vem em aumento, considerando o crescimento da necessidade de segurança física. Os dados estão repletos de brechas de seguridade de rede, particularmente na internet, onde transações fraudulentas e roubos de identidade são feitos por hackers que acessam as bases de dados com informações pessoais. Uma ameaça clara existe para a seguridade tanto de redes corporativas como governamentais.

Para reduzir o risco de ataques de hackers e brechas na seguridade, houve um aumento na implementação de tecnologias desenhadas para prover acesso seguro aos recursos da rede. Tal tecnologia está enfocada a ajudar o acesso ao controle dos operadores de rede, disponibilizando-a, somente, para aqueles indivíduos a quem o operador da rede deseja permitir o acesso. O acesso é controlado por dois processos: autenticação e autorização.

A autenticação é o processo pelo qual um indivíduo prova que ele é a pessoa a quem a credencial foi originalmente emitida por alguma organização terceirizada de confiança, quem confirmou originalmente a identidade do indivíduo. Por exemplo, se um cartão de identificação com foto foi emitido a John Doe, então John Doe se autentica ao apresentar o cartão, que correspondendo com a foto do seu rosto. A autenticação comprova que uma pessoa é o indivíduo identificado pela credencial.

A autorização é o processo pelo qual a um indivíduo autenticado é permitido o acesso aos recursos. Direitos de acesso podem ser outorgados de acordo com o posição do indivíduo dentro da organização, ou segundo a permissão ou não do operador de rede.

A tecnologia de cartão inteligente permite uma variedade de mecanismos para o suporte de autenticações.

¹³ Case studies illustrating the use of smart cards for logical access can be found on the Smart Card Alliance web site, www.smartcardalliance.org.

Proteção de PIN/Senha

Um esquema comum para conseguir autenticação envolve armazenar um PIN ou uma senha em um cartão inteligente. Quando um usuário queira obter acesso a um recurso da rede (um computador local, um servidor, uma aplicação de rede “web”, ou uma aplicação de intranet/extranet), o usuário ingressa o PIN, o qual é comparado ao PIN armazenado no cartão inteligente. Se eles são compatíveis o usuário é autenticado e pode acessar o recurso desejado. O serviço de controle de acesso do PIN usa autenticação de dois fatores para oferecer formas relativamente simples de assegurar que a pessoa certa está acessando um recurso.

Para apoiar o serviço de controle de acesso do PIN, pacote de software estão disponíveis que permitem um usuário administrar o PIN guardado no cartão. Por exemplo, este software (chamado algumas vezes “middleware”) pode permitir o PIN a ser modificado com o tempo, desativar o PIN se ingressado incorretamente certo número de vezes, e desbloquear o PIN se desativado por acaso.

Suporte PKI

O uso de certificados digitais que servem como parte de um PKI para prover um identificador digital único (“passaporte digital”), para cada usuário individual, é uma outra forma de facilitar a autenticação do usuário.

Esses certificados e chaves dos quais são derivados (que são armazenados na memória do circuito integrado ou “chip” do cartão inteligente) podem, então, ser usados para realizar uma operação de assinatura digital (depois que um processo de registro seja designado para provar a identidade exata da pessoa a quem se expede o certificado). A operação liga criptograficamente a pessoa que leva o cartão inteligente ao certificado. O cartão de identidade inteligente, geralmente, usa uma senha ou biométrie para “destrancar” o cartão afim de realizar a operação de assinatura digital solicitada.

Cada vez mais certificados são utilizados para apoiar a autenticação de redes de computadores onde o PKI há sido implementado. Por exemplo, Windows®2000, Windows®XP, e Windows® NT proporcionam suporte básico para um acesso seguro (como foi expedido pela Microsoft Certificate Authority). A armação atual do DoD CAC utiliza certificados separados para apoiar as assinaturas digitais e o acesso às redes para que não se deneguem as operações.

Um circuito integrado ou “chip” com base em um cartão inteligente pode armazenar chaves privadas de forma segura. As chaves privadas são a metade dos pares de chaves privadas do público, que são desenvolvidas para prover a funcionalidade criptográfica que permite as aplicações PKI como assinaturas digitais e criptografia de correio eletrônico ou “email”. Ademais, alguns chips são desenhados para gerar os pares de chaves privadas do público no mesmo cartão inteligente. Ao gerar o par de chaves no cartão, agrega um nível de seguridade à chave privada, uma vez que a mesma jamais precisa ser importada ao cartão desde outra fonte. A chave pública é enviada à autoridade de certificação, onde o certificado é criado para a sua distribuição, e enviado ao cartão inteligente para um armazenamento seguro.

Suporte de Chave Simétrica (Senhas de Uso Único)

Algumas organizações podem não estar em condições de justificar investimentos em sistemas de escala completa PKI, mas mesmo assim podem requerer um processo de autenticação mais forte para o acesso às redes de sistemas. As autenticações mais fortes podem ser realizadas por meio do uso de esquemas de chaves simétricas e pela gerência de senhas dinâmicas ou estáticas. Neste cenário, um PIN é combinado criptograficamente com uma chave compartilhada secreta (e potencialmente outro dado, tal como a data ou o tempo) para criar um código digital. O código é então comparado com um código gerado pelo provedor de serviço de rede de uma forma similar. Se os dois códigos são compatíveis, se considera o usuário autenticado.

Um cartão inteligente é capaz de armazenar, seguramente, um código secreto que pode ser usado para autenticar um usuário quando a chave é comparada a uma chave secreta operada pelo operador de rede. Esta simples compatibilidade prove certo nível de segurança, desde que o cartão do usuário somente pode suportar a chave secreta quando ela é emitida pelo operador de rede. A fragilidade deste esquema é que se a chave secreta é comprometida o usuário pode facilmente ser personificada. A efetividade do uso de chaves ou senhas estáticas reside na resistência ao ser manipulada ou qualidade “tamper-resistant” (sistema anti-roubo) do chip do cartão inteligente para proteger a chave ou a senha do hacker. Algumas organizações utilizam esquemas do tipo rotação de chave ou “key rotation” ou o posicionamento de chave ou “key versioning” para dificultar o comprometimento do sistema.

Um esquema auxiliar serve para gerar uma chave ou uma senha de forma dinâmica. Neste esquema, cada transação tem uma chave diferente a qual pode, então, ser usada por ambos os lados da transação para assegurar a segurança. Os cartões inteligentes podem apoiar este processo, usando o poder computacional do chip para criar chaves ou a senha dinâmica.

Suporte biométrico

Outro uso importante e em aumento do cartão inteligente é a autenticação baseada em biométrie¹⁴.

O cartão inteligente armazena informação biométrica de um indivíduo e é autenticado em tempo real. Os chips de cartões inteligentes podem armazenar virtualmente qualquer tipo de informação biométrica, dependendo do tamanho da memória, que pode ser em um formato digital comprimido (por exemplo, minúcias de impressão digital), ou como uma representação digital completa da característica biométrica (uma imagem digital).

A autenticação biométrica requer que o indivíduo forneça a característica biométrica única particular a um leitor ou dispositivo de escaneamento ou “scanning device”. O dispositivo recolhe o dado biométrico e o compara com aquele armazenado no cartão inteligente. Sendo eles compatíveis, se considera, então, o indivíduo a autenticado.

A adição de autenticação biométrica com base em cartão inteligente pode aumentar a seguridade a níveis bastante altos. O cartão inteligente usa para autenticações três fatores, tomando algo que o usuário tem (a credencial de

14 Para mais informação sobre o uso de biométricos com cartões inteligentes, ver o Smart Card Alliance Report, “Smart Cards and Biometrics in Privacy-Sensitive Secure Identification Systems”, publicado em Maio de 2002.

cartão inteligente), algo que o usuário sabe (um PIN ou uma senha) e algo que o usuário é (um ou mais dados biométricos). Em alguns casos, um dado biométrico pode ser usado em vez de um PIN para o processo de autenticação de dois fatores que oferece um acesso mais seguro dos dados no cartão.

O último sistema de acesso físico utiliza técnicas de "match on card", onde o leitor recolhe o dado biométrico e o envia ao cartão. O cartão então compara o dado biométrico adquirido com o que está armazenado no cartão e diz pro leitor se os dados biométricos são compatíveis. Este processo, posteriormente, melhora a seguridade de um sistema, uma vez que os dados biométricos originais nunca são expostos e, como resultado, não podem ser capturados.

Resumo do Acesso Lógico

Um cartão inteligente de acesso físico pode aportar uma melhor autenticação do cartão de identificação e do usuário (por meio do uso de impressões digitais, dados biométricos, e tecnologias de senha / PIN), permitir a não denegação de transações, e a criptografia do e-mail. Se uma companhia busca esses benefícios como parte dos seu plano completo de segurança de rede, eles podem ser incorporados ao negocio, como uma tecnologia de cartão inteligente que abarque tanto o acesso físico, como o lógico.

Um número crescente de corporações, tanto dos setores públicos como privados, estão adotando cartões inteligentes para suportar o acesso físico e lógico em um cartão. Por exemplo: a Microsoft está emitindo uma credencial de empregado que além de usar-se para a abertura de portas com uma interfase sem contato, também permite o registro seguro da rede, utilizando uma aplicação que se encontra no chip de contato incluído no cartão.

Atualmente, a separação histórica da segurança física e de rede é o maior obstáculo para o desenvolvimento do mercado de cartões ID que suporta o acesso físico e lógico. Essas duas funções, geralmente, são realizadas por duas partes diferentes de uma organização, cada uma com uma missão, pressuposto e infra-estrutura técnica separadas. No entanto, como a tecnologia há tornado-se mais, amplamente, disponível em formas variadas (por exemplo: com contato, sem contato, USB), mais corporações estão desenvolvendo negócios que requerem a integração dessas duas funções de seguridade para alcançar diminuições de gastos e para melhorar a seguridade abrangente da corporação.

Payment Support Suporte de Pagamento

Um cartão inteligente que permite o controle do acesso físico pode suportar transações de pagamento, seja, através de uma interface de contato ou sem contato. Um exemplo é o cartão SmarTrip, um cartão inteligente sem contato usado pelo sistema de transporte WMATA. Os passageiros carregam uma quantia "x" no cartão e então usam o para acessar o metrô através das portas giratórias de entrada, as quais deduzem, automaticamente, o valor do passagem, da quantia existente no cartão.

Enquanto o uso da tecnologia de cartão inteligente tem sido pioneiro no ambiente do transporte, onde a combinação de pagamento seguro e rápido controle de acesso físico são requerimentos máximos, pagamentos apoiados por cartões de contato estão começando a aparecer no setor

comercial dos Estados Unidos. Os programas pilotos *Master Card Pay Pass* e o *American Express Express Pay* usam tecnologias sem contato para efetuar transações de pagamento seguras de cartões de créditos.

Os pagamentos podem ser realizados por um chip (micro-circuito) de contato integrado no mesmo corpo do cartão, assim como chip sem contato usado para o acesso físico. Atualmente, os chips de contato, podem suportar uma ampla variedade de aplicações de pagamento, desde bolsas eletrônicas nas quais valores monetários podem ser contidas, até transações convencionais de crédito/ débito. Uma especificação global chamada EMB se criou de forma que os cartões inteligentes possam apoiar transações de débito e crédito com base em chip, exatamente como os cartões de fita magnética o fazem hoje em dia.

Uma aplicação do cartão inteligente que foi desenhada, ao começo, para apoiar, unicamente, o controle do acesso físico, poderia incluir uma aplicação adicional para apoiar, também, uma variedade ampla de funções de pagamento. A combinação dessas funções poderia resultar em uma proposta mais forte para adoção da tecnologia de cartão inteligente. Por exemplo, o banco de uma corporação poderia prover um cartão inteligente corporativo aos empregados, o que melhoraria a função de pagamento do banco, assim como, também, um chip sem contato usado para o acesso físico das instalações corporativas. Neste caso, a corporação poderia aumentar, potencialmente, seus benefícios financeiros ao não ter que usar dois programas separados de cartões, e também poderia reduzir, provavelmente, alguns dos custos de administração do programa de acesso físico.

Um cenário típico (e o que já tem sido implementado em várias universidades e empresas) é o tão conhecido "campus card". Este é um cartão inteligente múlti-função que pode ser usado como um cartão de identidade (que inclui uma foto) e pode ser usado para pagar as refeições e as máquinas vendedoras automáticas, abrirem as portas dos dormitórios, retirar livros da biblioteca, e para pagar por ligações telefônicas. Geralmente, esses cartões empregam uma série de tecnologias, tais como fitas magnéticas, código de barras, e micro-circuitos de cartão inteligente que abarcam uma ampla gama de aplicações funcionais. A maioria das implementações suportam o controle do acesso físico em combinação com aplicações de pagamento e uma variedade de outras aplicações, as quais agregam valor ao cartão.

Armazenamento Seguro de Dados

Quando a habilidade da tecnologia de cartão inteligente de prover armazenamento seguro e portátil de dados é agregada à capacidade computacional do chip, o resultado final é um aparelho de computação dinâmico e portátil, que pode abarcar uma variedade ampla de aplicações em forma segura. Os únicos contratempos técnicos são o tamanho físico do micro-circuito (chip) e a quantidade de memória disponível.

Por esta razão os cartões inteligentes estão sendo usados de várias formas inovadoras, apoiando funções que envolvem o armazenamento portátil e seguro de informação delicada e não delicada. Por exemplo, históricos médicos podem ser armazenados em um cartão inteligente, de tal forma que somente o portador do cartão ou o seu doutor poderam acessar tais

historiais. O acesso de dados está, geralmente, protegido por um tipo lógico de controle de acesso, como um PIN.

Igualmente, o DoD CAC emitido aos militares incluem severas aplicações de armazenamento seguro que agrupam a informação pessoal de cada portador do cartão. A CAC pode potencialmente armazenar informação relacionada ao histórico médico ou outro dado relevante da missão da pessoa.

Os cartões de contato usados para sistemas de acesso físico podem armazenar com segurança informação que rastreia o uso do cartão. Por exemplo um cartão sem contato pode ser usado para gravar quando o portador do mesmo ingressa a um edifício em particular (por exemplo, lugar, data e tempo da porta) para registro e auditoria. Esta função pode ser administrada pelo cartão ou por um servidor central dependendo da infraestrutura e requerimentos da corporação.

Resumo

O objetivo de apoiar a adoção de cartões inteligentes para controlar de acesso físico pode ser, enormemente, melhorado pela identificação dos aspectos e funções adicionais, apoiados pela plataforma de cartão inteligente. A funcionalidade adicional pode usar a interfase sem contato que suporta acesso físico, um chip e uma interfase sem contato dedicada a uma aplicação diferente, ou um chip de contato, adicional, incluído na estrutura do cartão inteligente.

Qualquer desenvolvimento de um programa de cartão inteligente deveria, assim, incluir um análise de outras funções que possam estimular o investimento do cartão inteligente. Através deste processo uma corporação pode revelar benefícios adicionais de migrar para uma tecnologia de cartão inteligente que resultaria na redução de gastos para a corporação ao mesmo tempo em que simplifica o processo de negócios e melhora a conveniência do usuário.

Conclusão

O governo e a indústria estão levando a cabo importantes atividades para implementar novos sistemas de controles de acesso, para verificar os privilégios e a identidade de uma pessoa antes de dar-lhe acesso físico (a um lugar ou um edifício) ou acesso lógico (para informação ou outras fontes em linha ou “online”). Entre os requerimentos-chaves para esses sistemas encontramos um maior controle de acesso seguro, conveniência do usuário melhorada, processos de verificação de identidade simples, e custos gerais de administração e de gerência mais baixos.

Muitas agências do governo federal estão implementando sistemas de controles de acesso lógico e físico com bases em cartões inteligentes, com seus esforços dirigidos a implementação de tecnologia de padrões base. Como parte desse esforço, iniciativas de agências cruzadas do governo, operadas pela GSA e a NIST, estabeleceram especificações para interoperabilidade através das implementações governamentais. Corporações comerciais como a Sun e a Microsoft estão implementando sistemas de controle de acesso baseadas em cartões inteligentes para gerenciar o acesso global de empregados aos recursos corporativos.

O desenho de um sistema de acesso físico seguro inclui considerações adicionais ao escolher a credencial e o leitor. O desenho de um sistema apropriado requer uma definição completa dos requerimentos do sistema, incluindo uma política de segurança e de funcionalidade necessárias, e deve considerar fatores tais como custo, requerimentos para integrar e migrar desde sistemas legais, e o efeitos da implementação na organização e nos usuários.

Ambas as tecnologias de cartão inteligente com ou sem contato estão sendo usadas em sistemas de controles de acesso. A tecnologia de cartão inteligente oferece muitos benefícios para um sistema de controle de acesso, incluindo:

- Alta velocidade de acesso e custos de manutenção reduzidos para o controle do acesso físico sem contato.
- Segurança mais forte que apoie a autenticação de múltiplos fatores e uma variedade de técnicas de autenticação e criptografia.
- Flexibilidade para incorporar múltiplas aplicações e apoiar múltiplas tecnologias de cartões e leitores.
- Estabelecimento de soluções com base em padrões que oferecem alternativas de componentes interoperativos e disponibilidade de cartões e leitores de diversos vendedores.

A convergência das necessidades do governo e do setor comercial e a disponibilidade de alternativas seguras de cartões inteligentes, estão levando à implementação de sistemas de controle de acesso com base em cartões inteligentes. A tecnologia de cartões inteligentes permite que o sistema de controle de acesso possa implementar mecanismos de verificação de identidade mais seguros, tanto para o acesso físico como lógico, e oferecer uma plataforma tecnológica para acrescentar novas aplicações que melhorem ainda mais a conveniência do usuário e simplifique os processos do negócio.

Para maior informação sobre cartões inteligentes e o papel que tem as aplicações de identificação segura e outras, favor visitar o website da Smart Card Alliance em www.smartcardalliance.org ou contatar diretamente ao Smart Card Alliance ao 1-800-556-6828.

Referências e Recursos

"Access Control Technologies for the Common Access Card," a study by the Security Equipment Integration Working Group (SEIWG), April 2002

"Amex Opts for Biometric RFID Card," *RFID Journal*, February 17, 2003

"Building Blocks of the U.S. Smart Card Market," *Card Technology*, May 2003

"California Independent System Operators (CalISO) secures access to electric power grid control with smart cards and PKI," Smart Card Alliance case study

"Contactless Smart Card Technology for Physical Access Control," Avisian, Inc. report, April 1, 2002

"Contactless Technology for Secure Physical Access: Technology and Standards Choices," Smart Card Alliance report, October, 2002

"Department of Defense to issue 13 million Common Access Cards," Smart Card Alliance case study

"Dutch bank deploys 33,000 smart cards to authenticate internal users and secure online transactions," Smart Card Alliance case study

"Federal Deposit Insurance Corporation deploys smart cards and PKI to internal staff and field agents," Smart Card Alliance case study

"Microsoft employees to use smart card access controls," Paul Roberts, *IDG News Service/Boston Bureau*, www.idg.net, September 23, 2002

"Navy's DENCAS system centralizes dental records and secures access with smart cards and PKI," Smart Card Alliance case study

"A Primer to the Implementation for Smart Card Management and Related Systems," Global Platform, www.globalplatform.org

"Physical Security Bridge to IT Security," Open Security Exchange, www.opensecurityexchange.com

"Schlumberger/SEMA deploys 89,000 smart cards and PKI to protect corporate and customer data," Smart Card Alliance case study

"Shell Group's info security centers around 85,000 smart cards with PKI and single sign-on for smart card-enabled PKI," Smart Card Alliance case study

"Smart Cards and Biometrics in Privacy-Sensitive Secure Identification Systems," Smart Card Alliance report, May, 2002

Reconhecimentos da Publicação

Este informe foi desenvolvido pela Smart Card Alliance para oferecer um manual sobre sistemas de identificação de acesso físico seguro e para discutir como estes sistemas estão migrando à tecnologia de cartões inteligentes. A publicação deste documento pela Smart Card Alliance não implica o endosso de nenhuma organização membro da Aliança.

A Smart Card Alliance deseja agradecer aos membros do grupo de trabalho de Identificação pessoal segura pelos seus comentários e contribuições. Participantes de 28 organizações, tanto públicas como privadas se involucraram no desenvolvimento deste informe, incluindo: ACI Worldwide, ActivCard, ASSA ABLOY ITG, Bell ID, Datacard Group, eID Security, EDS, Gemplus, Hitachi America Ltd., Honeywell Access Systems (OmniTek), IBM, ISR Solutions, LaserCard Systems, MasterCard International, MGM Security Consulting, NASA, Northrop Grumman Information Technology, SC Solutions, Schlumberger, SCM Microsystems, Smart Commerce Inc., Transportation Security Administration, Unisys, U.S. Dept. of Defense, U.S. Dept. of Homeland Security, U.S. Dept. of State, U.S. Dept. of Transportation/Volpe Center, XTec Incorporated.

Agradecimento especial às pessoas que escreveram, revisaram e/ou editaram este informe .

Tim Baldrige, NASA

Dovell Bonnett, ASSA ABLOY ITG

Kirk Brafford, ActivCard

Joe Broghamer, U.S. Dept. of
Homeland Security

Mike Davis, Honeywell Access
Systems (OmniTek)

Mike Dinning, U.S. Dept. of
Transportation/Volpe Center

Kevin Kozlowski, XTec Incorporated
Lolie Kull, U.S. Dept. of State

Philip Lee, SC Solutions

Mark McGovern, MGM Security
Consulting

John McKeon, IBM

Cathy Medich, Consultant and
Task Force Chair

Bob Merkert, SCM Microsystems

Dwayne Pfeiffer, Northrop
Grumman Information Technology

Tate Preston, eID Security

J. C. Raynon, SCM Microsystems
James Russell, MasterCard
International

James Sharp, Transportation
Security Administration

Randy Vanderhoof, Smart Card
Alliance

Mike Vermillion, EDS

Tim Weisenberger, U.S. Dept. of
Transportation/Volpe Center

Chuck Wilson, Hitachi America Ltd.

Direito de Autor (Copyright Notice)

Copyright 2003 Smart Card Alliance, Inc Todos os direitos reservados

Marcas Registradas (Trademark Notices)

Todas as marcas registradas são propriedade dos seus respectivos donos.

Apêndice A: Definição de Termos e Siglas

Formato de sistema de controle de acesso

O formato de sistema de controle de acesso se refere ao padrão bit que o leitor transmite ao painel de controle. O formato especifica quantos bits formam o fluxo de dados e o que estes bits representam. Por exemplo, os primeiros bits podem transmitir o código do estabelecimento, os seguintes um número de identificação único, os próximos uma paridade, e assim por diante.

AES

“Advanced Encryption Standard” (Padrão avançado de criptografia).

Barium ferrite

Tecnologia magnética que usa “barium ferrite” na composição da credencial de identificação para armazenar dados e fazer que os mesmos estejam disponíveis para o dispositivo de leitura.

Biométrico(a)

Tecnologias biométricas são definidas como métodos automatizados de identificação ou autenticação de identidade de uma pessoa viva com base nas características fisiológicas ou de comportamento únicas.

CCTV

“Closed Circuit Televisión” (Circuito Fechado de Televisão)

Chip

Componente eletrônico que realiza funções lógicas de processamento e/ou memória.

Coabitação

É a habilidade de que múltiplas tecnologias residam no mesmo cartão e não interfiram umas com as outras (por exemplo, um cartão de tecnologia múltipla).

Cartão Inteligente de Contato

É um cartão inteligente que se conecta ao dispositivo de leitura através de um contato físico direto entre o chip do cartão inteligente e o leitor do cartão (ver ISO/IEC 7816).

Cartão Inteligente sem Contato

É um cartão inteligente cujo chip se comunica com o leitor usando radio frequência e não requer contato físico com o leitor do cartão.

Painel de Controle

É o componente do sistema de controle de acesso que se conecta a todos os leitores de porta de acesso, fechaduras de portas e o servidor de controle de acesso. O painel de controle valida o leitor e aceita os dados. Dependendo do desenho geral do sistema, o painel de controle pode enviar os dados ao servidor de controle de acesso ou pode ter suficiente inteligência local para determinar os direitos do usuário e dar a autorização final de acesso. O painel de controle pode ser chamado de controlador ou painel.

Credencial

É o dispositivo de identificação geral (tanto o dispositivo físico como os dados contidos nele). Comumente conhecido como a “ficha de identificação” (ID token) nos sistemas de controle de acesso físico.

DES

“Data Encryption Standard” (Padrão de Criptografia de Dados).

Leitor de porta de acesso

É o dispositivo em cada porta, que se comunica com um cartão ou credencial de identificação, e envia dados do cartão ao painel de controle para decidir sobre os direitos de acesso.

Fechadura Eletrônica (“Door strike”)

É a fechadura eletrônica em cada porta, que está conectada ao painel de controle.

DSA

“Digital Signature Algorithm” (Algoritmo de assinatura digital).

Cartão de interfase dupla

É um cartão de identificação que tem um único chip de cartão inteligente com duas interfases – uma interfase de contato e uma interfase sem contato – usando memória e recursos do chip compartilhado.

Campo de recepção

É o campo de radio frequência ou eletromagnético transmitido constantemente pelo leitor da porta sem contato. Quando um cartão sem contato está no raio de ação do campo de recepção, a antena interna do cartão converte o campo de energia em eletricidade que prove de energia ao chip. O chip, então, usa a antena para transmitir dados ao leitor.

ECC

“Elliptic Curve Cryptography” (Criptografia de curva elíptica).

EMV

Europay MasterCard Visa. Especificações desenvolvidas pela Europay, MasterCard e Visa que definem um conjunto de requerimentos que asseguram a interoperabilidade entre cartões com chip de pagamento e os terminais.

FCC

“Federal Communications Commission” (Comissão Federal de Comunicações).

FIPS

“Federal Information Processing Standard” (Padrão Federal de Processamento de Informação).

GSA

“General Services Administration” (Administração de Serviços Gerais).

GSC-IS

“Government Smart Card Interoperability Specification” (Especificação Governamental de Interoperabilidade de Cartões Inteligentes). O GSC-IS foi definido para oferecer a habilidade de desenvolver cartões inteligentes de identificação segura que possam funcionar através de múltiplas agências do

governo ou entre os governos Federal, Estadual e Local, e oferece soluções a vários problemas de interoperabilidade associados com a implementação da tecnologia de cartões inteligentes de contato. Uma próxima revisão do GSC-IS (manejada pelo NIST) incluirá definições de interoperabilidade para tecnologias de cartões inteligentes sem contato.

Sistema de cabeça de Rede (“Head-end system”)

É o servidor de controle de acesso, o software e as bases de dados usados em um sistema de controle de acesso físico.

Cartão Híbrido (“Hybrid card”)

É um cartão de identificação que tem dois chips de cartão inteligente –um chip de contato e um sem contato – que não estão interconectados.

IDEA

“International Data Encryption Standard” (Padrão Internacional de Criptografia de Dados).

IEC

“International Electrotechnical Commission” (Comissão Internacional Eletro técnica).

Circuito Integrado

Ver chip.

ISO

“International Organization for Standardization” (Organização Internacional de Padronização).

ISO/IEC 14443

Padrão ISO/IEC para “Cartões de Identificação – Cartões com Circuitos Integrados sem contato – Cartões de Proximidade”.

ISO/IEC 15693

Padrão ISO/IEC para “Cartões de Identificação – Cartões com Circuitos Integrados sem contato – Cartões de Vizinhança (Vicinity Cards)”.

ISO/IEC 7816

Padrão ISO/IEC para cartões de circuito integrado de contato.

Acesso Lógico

É o acesso a recursos “on-line” (por exemplo, redes, arquivos, computadores, bases de dados).

MCU

Ver micro controlador.

Micro controlador (MCU)

É um chip de computador altamente integrado que contém todos os componentes compreendidos em um controlador. Tipicamente, isto inclui um CPU, RAM, alguma forma de ROM, portas de I/O e registradores de tempo. À diferença de um computador de uso geral, um micro controlador está desenhado para operar num ambiente restringido.

Migração

É o movimento planejado e incremental de um sistema de controle de acesso físico existente a um sistema com base em cartões inteligentes.

Cartão de Aplicação Múltipla

É uma identificação de cartão inteligente que executa múltiplas aplicações – por exemplo, acesso físico, acesso lógico, armazenamento de dados e bolsa eletrônica (electronic purse) – usando um único cartão.

Leitor de Fatores Múltiplos

É um leitor de cartões inteligentes que inclui um teclado de PIN, um leitor biométrico ou ambos, para permitir a autenticação de múltiplos fatores.

Cartão de Tecnologia Múltipla

É um cartão de identificação que tem duas ou mais tecnologias de identificação que são independentes e que não interagem ou interferem uma com a outra. Um exemplo é um cartão que contém um chip de cartão inteligente e uma fita magnética.

Leitor de Tecnologia Múltipla

É um cartão de leitura/escritura que pode acomodar mais de uma tecnologia de cartão num mesmo leitor (por exemplo, tecnologias de cartões sem contato, tanto ISO/IEC 14443 como ISO/IEC 15693 ou tecnologias sem contato, tanto de 13.56 MHz como 125 kHz).

NIST

“National Institute of Standards and Technology”(Instituto Nacional de Padrões e Tecnologia).

Não Repúdio (“Non-repudiation”)

É a habilidade de certificar-se e de ter a evidência de que uma ação específica ocorreu numa transação eletrônica (por exemplo, que o criador de uma mensagem não possa negar haver enviado uma mensagem ou que um participante numa transação não possa negar a autenticidade da sua assinatura).

Raio de ação operacional (Operational range)

É a distância do leitor na qual a credencial de identificação sem contato é efetiva.

PC

“Personal computer”(Computador pessoal).

Acesso Físico

É o acesso a estabelecimentos físicos (por exemplo, edifícios, quartos, aeroportos, depósitos).

PIN

“Personal Identification Number”. (Número de identificação pessoal). É um código numérico que está associado com um cartão de identificação e que acrescenta um segundo fator de autenticação ao processo de verificação de identidade.

PKI

“Public Key Infrastructure” (Infra-estrutura de Chave Pública).

RF

“Radio Frequency” (Radio Freqüência).

RFID

“Radio Frequency Identification” (Identificação de Radio Freqüência)

RSA

Refere-se à tecnologia de criptografia de chave público-privada que utiliza um algoritmo desenvolvido por Ron Rivest, Adi Shamir y Leonard Adleman, que pertence e que está sob a licença de RSA Security.

Cartão Inteligente

Um cartão inteligente inclui um chip integrado que pode ser, ou um micro controlador com memória interna, ou um chip de memória unicamente. O cartão se conecta a um leitor com contato físico direto ou com interfase eletromagnética remota sem contato. Com um micro controlador, os cartões inteligentes têm a habilidade única de armazenar grandes quantidades de dados, executar suas próprias funções no cartão (por exemplo, criptografia e assinaturas digitais) e interagir inteligentemente com o leitor de cartão inteligente.

Cartão de Identificação Inteligente (“Smart ID card”)

Um cartão de identificação que é um cartão inteligente.

3DES

“Triple DES” (DES Triplo).

UL

“Underwriters Laboratories” (Laboratórios Subscritos).

USB

“Universal Serial Bus” (Barramento Serial Universal).

Tecnologia Wiegand

A tecnologia Wiegand é amplamente usada para aplicações de acesso físico, e inclui uma interfase, um sinal, um formato de 26 bits, um efeito eletromagnético e uma tecnologia de cartão. Uma fita Wiegand é a implementação da tecnologia Wiegand numa credencial de identificação.

Fiação Lógica (“Wired logic”)

É um cartão sem contato que tem um circuito eletrônico que está desenhado para uma função específica (por exemplo, segurança, autenticação) sem um MCU integrado.