



Cartões Smart e Sistemas de Identificação Seguros: Construindo uma Cadeia de Confiança

Um briefing da Smart Card Alliance Latin America (SCALA)

Data da publicação: Julho 2005

Data da modificação: Outubro 2006-10-30

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

Sobre a Aliança de Cartões Smart da América Latina (SCALA)

A Aliança de Cartões Smart da América Latina (SCALA, sigla em inglês) é uma organização sem fins lucrativos, apolítica, que lidera uma associação de firmas multi-industriais que trabalham em prol da aceleração da aceitação da tecnologia de cartão smart para aplicações múltiplas. Entre os membros da aliança encontram-se líderes em áreas como bancos, serviços financeiros, computadores, telecomunicações, acesso físico, transporte, tecnologia, serviços de saúde, comércio varejista e indústria do entretenimento, bem como um número de agências governamentais. Através de projetos específicos, como programas educacionais, pesquisa de mercado, advocacia, relações industriais e fóruns abertos, a aliança mantém seus membros conectados aos líderes da indústria e inovadores do pensamento. A aliança é a única voz da indústria de cartões smart nos EUA e na AL. Para mais informação, visite: www.smartcardalliance.org

Reconhecimentos desta Publicação

Este informe é baseado no conteúdo do documento da Aliança Smart Card, "Sistemas de ID seguros: Construindo uma cadeia de confiança", que foi desenvolvido pela força tarefa da Aliança Smart Card para segurança da informação pessoal, publicado em março de 2004. A publicação deste documento pela Smart Card não implica a aprovação de qualquer das organizações-membro da Aliança.

A Aliança Smart Card deseja agradecer aos membros da força tarefa da Aliança Smart Card para segurança da informação pessoal por sua contribuição. Participantes de 23 organizações estiveram envolvidos no desenvolvimento do documento original, dentre eles: ActivCard, Alegria Technologies, AOS Hagenuk, ASSA ABLOY ITG, Atmel Corporation, Gemalto, BearingPoint, Datakey, Datatrak Information Services, Inc., EDS, eID Security, Gemplus, IBM, Identix, Infineon Technologies, LaserCard Systems, Lockheed Martin, MartSoft Corporation, Northrop Grumman Information Technology, Philips Semiconductors, Smart Commerce, Inc., Unisys, U.S. General Services Administration.

Direitos autorais © 2005 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, integridade ou adequação da informação deste informe.

Introdução

A demanda por seguridade é uma das exigências mais recorrentes em nossa sociedade. O desafio é simples: como proteger aquilo que pertence a você. “Você” pode ser uma organização, uma agência governamental ou um indivíduo. O que pertence a você pode ser algo tangível, como um objeto físico, ou algo intangível, como dados, direitos e privilégios. Mas qualquer que seja o caso, esses bens tem valor significativo para seu proprietário.

Virtualmente tudo aquilo de que os bens devam ser protegidos envolve a presença de pessoas. Ataques digitais e físicos são criados e perpetrados por pessoas. Portanto é essencial poder identificar clara e definitivamente aquelas pessoas que devem ter acesso ao que pertence a você, e permitir-lhes este acesso. Todos os demais devem ser barrados. Tal capacidade de identificação somente é possível em um sistema de identificação (ID) seguro.

Essencial para um sistema de identificação seguro é a *cadeia de confiança*. Confiança nos processos, nas pessoas, na arquitetura e tecnologia são vitais para a construção e a confiança em um sistema de ID seguro. A cadeia de confiança garante a autenticidade das pessoas, das organizações emissoras, dispositivos, equipamentos, redes, e outros componentes de um sistema ID seguro. A cadeia de confiança também precisa assegurar que a informação dentro do próprio sistema seja verificada, autenticada, protegida e usada adequadamente.

O uso de objetos de ID com capacidade inteligente, especialmente na forma de cartões smart, oferece vantagens tanto para a segurança física como lógica. Estes cartões são um elo vital na cadeia de confiança. Eles oferecem verificação de identificação segura e acurada, e, combinados com outras tecnologias de sistemas de ID, como biométricos e certificados digitais, podem reforçar a segurança do sistema e proteger a privacidade da informação.

O poder e a portabilidade do cartão smart, uma arquitetura bem projetada e regras operacionais restritas, quando combinadas, formam uma cadeia de confiança confiável e controlável para sistemas seguros de ID.

O que torna seguro um sistema de identificação

Um sistema de identificação seguro é projetado para atender a um requerimento básico: verificar que um indivíduo é o indivíduo que ele alega ser. Quando projetado corretamente, um sistema de ID seguro implementa uma cadeia de confiança pela qual todos os envolvidos ficam certos de que o indivíduo apresentando um cartão ID é a pessoa que detém as credenciais do cartão e que estas credenciais são válidas. (O termo credencial neste artigo se refere à informação guardada no cartão e representa o documento de identidade do indivíduo e seus privilégios). Um sistema de ID seguro pode prover um indivíduo com credenciais confiáveis que podem ser usadas numa variedade de aplicações, desde permitir acesso a prédios ou redes até comprovar o direito a serviços ou para conduzir transações *online*.

O cartão ID¹ é peça central em qualquer sistema de ID seguro. Este é usado como uma representação portátil, confiável e verificável da identidade e direitos e privilégios de um indivíduo dentro do sistema ID. Para que um cartão ID tenha esses requerimentos, o sistema ID deve assegurar que o cartão tenha sido emitido por uma autoridade legítima, que o cartão ID e as credenciais nele contidas não foram falsificadas ou adulteradas, e que a pessoa portadora do cartão ID corresponde ao indivíduo que foi registrado no sistema ID.

O modelo de confiabilidade do sistema ID seguro

Sistemas de ID seguro podem ser implementados dentro de um único grupo, por grupos múltiplos dentro de uma organização ou empreendimento ou entre múltiplas organizações e empreendimentos. Independentemente do número ou tipos de entidades envolvidas, para serem realmente seguros, os sistemas ID precisam implementar um modelo de confiabilidade. O modelo de confiabilidade institucionaliza princípios e políticas básicos: as operações do sistema sempre terão o mesmo resultado, independentemente de onde elas forem realizadas e todas as partes envolvidas podem confiar que o sistema verifica as identidades com acuidade e segurança. Antes de implementar qualquer sistema, todas as organizações participantes devem definir e entrar em acordo a respeito do modelo de confiabilidade.

Elementos de projeto que tornam um sistema ID seguro

O projeto de sistemas ID seguros requer uma série de decisões que selecione e implemente políticas, procedimentos, arquitetura, tecnologia e equipe. O projeto precisa implementar o nível desejado de segurança e a cadeia de confiança apropriada, com o processo de autenticação incorporando medidas de segurança e tecnologia para prevenir a falsificação e a falsidade ideológica, assim como assegurar a privacidade das credenciais do ID.

O projeto de um sistema ID seguro precisa incluir os seguintes aspectos:

¹ Este texto se refere ao objeto físico ID como um “ID” ou “cartão ID”. Enquanto sistemas ID podem emitir diferentes formatos físicos de ID, um cartão plástico que incorpore outras tecnologias usadas na identificação de aplicações (p. ex. chip, código de barras, tarja magnética) é o formato predominante para um sistema ID seguro.

-
- Um processo de registro seguro que estabeleça a identidade de cada indivíduo e determine que a pessoa está investida dos privilégios que lhe são outorgados;
 - Procedimentos para emitir cartões ID com segurança e assegurar que os IDs são emitidos apenas por organizações autorizadas e para a pessoa a quem se destina;
 - Políticas e procedimentos para monitoração do uso do ID;
 - Procedimentos para administração do ciclo de vida do ID;
 - Treinamento para usuários e emissores;
 - Políticas, procedimentos e tecnologias para proteger o acesso à informação sobre os portadores dos IDs no sistema;
 - Segurança dos controles para permitir que apenas pessoas autorizadas tenham acesso às informações do ID;
 - Processo de autenticação que implemente a linha de confiança definida, verificando a identidade dos portadores do ID e a legitimidade dos cartões e de suas credenciais.

Requisitos de privacidade para Sistemas ID seguros

Em adição a proteger os bens de uma organização, sistemas ID seguros também precisam proteger a privacidade dos indivíduos registrados no sistema e promover a salvaguarda de sua informação pessoal. Os requisitos de privacidade são um ponto chave para o sucesso da implementação de um sistema ID seguro. Para que um sistema de identificação seja considerado como habilitado para uma adequada privacidade, um sistema de identificação precisa satisfazer os seguintes requisitos:

- Controlar o armazenamento, uso e divulgação de informações pessoais;
- Proteger o direito de cada indivíduo de controlar como a informação pessoal será coletada e promulgada;
- Proteger contra roubo de identidade e o uso da informação pessoal de um indivíduo para fins fraudulentos;
- Proteger a confidencialidade, integridade e disponibilidade da informação que identifica ou descreve um indivíduo.

Um número de organizações governamentais e grupos industriais desenvolveram recomendações para práticas justas de manuseio de informações e diretrizes para proteger a privacidade individual. Os projetistas de sistemas devem considerar as práticas de comércio, políticas de segurança, e arquitetura dos sistemas, bem como as tecnologias, ao desenvolverem um sistema que garanta a privacidade.

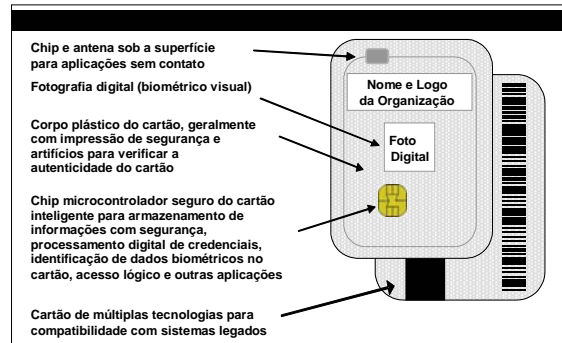
Cartões Smart e sistemas ID seguros

Os cartões smart são amplamente reconhecidos como uma das formas mais seguras e confiáveis de identificação eletrônica. Um cartão smart que tem embutido nele um chip de computador pode ser tanto um microcontrolador com memória interna como apenas um chip de memória. O cartão se conecta com um leitor com contato físico direto ou com uma interface eletromagnética remota sem contato. Com um microcontrolador embutido, os cartões smart têm a capacidade de armazenar grandes quantidades de informação, realizar

suas próprias funções de cartão (p.ex. codificar e assinatura digital) e interagir inteligentemente com um leitor de cartão smart.

Um cartão smart ID pode combinar várias tecnologias ID, incluindo chip, marcadores de segurança visual, tarja magnética, código de barras e/ou faixa ótica. Muitas organizações governamentais e empresas estão implementando sistemas de ID seguro baseados no cartão smart

para permitir acesso físico e lógico e acrescentando outras aplicações que tradicionalmente requeriam processos de identificação e cartões distintos.

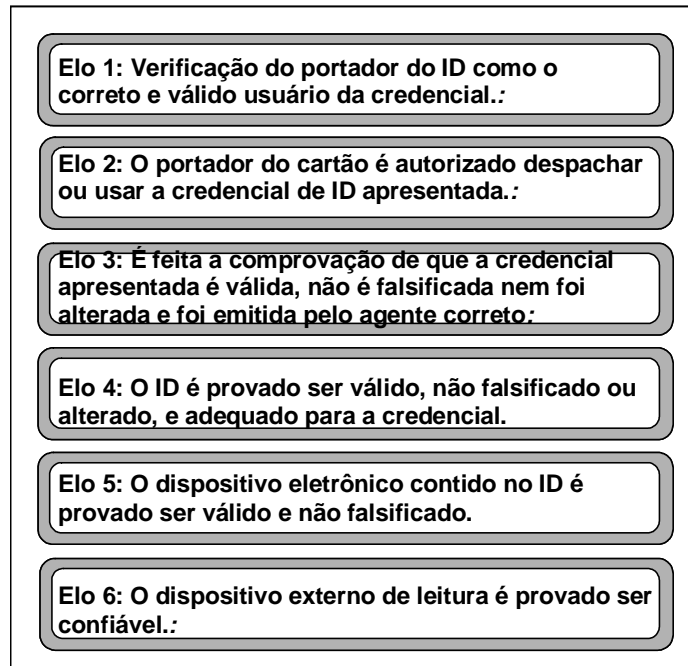


Uso de ID, a cadeia de confiança e o papel dos cartões smart

A cadeia de confiança num sistema ID seguro percorre a totalidade dos componentes e processos do sistema, assegurando que o sistema como um todo é merecedor de confiança.

Esta seção descreve a cadeia de confiança necessária para autenticar a identidade de um indivíduo e assegurar a validade do ID e credencial uma vez que um ID foi emitido e está em uso. Para ilustrar a cadeia de confiança mais forte possível, a discussão pressupõe que o ID inclua um dispositivo eletrônico (ou chip) inserido num documento pessoal portátil (por exemplo, um passaporte eletrônico) ou em um cartão.

A figura abaixo resume os elos-chave na cadeia de confiança de um sistema ID seguro durante o processo de autenticação quando o ID é usado.



Verificação Física da Identidade

A autenticação da identidade começa tipicamente pela verificação física do ID. IDs podem ser verificados fisicamente de várias maneiras. O método escolhido deve ser apropriado para o nível de confiança desejável. Os métodos incluem:

- Exame de uma identidade que é apresentada pelo usuário mas que não tem que ser entregue ao que a examina (como um passe-flash)
- Exame de um ID entregue pelo usuário
- Inspeção mecânica de dados únicos contidos no ID (tais como um código de barras) ou comparação de um ID com um padrão de referência.

Em todos os casos, o ID apresentado é checado visual ou eletronicamente por detalhes específicos que conferem sua autenticidade. Estes detalhes podem ter a forma de uma ou mais características de segurança, tais como:

- Correção da informação topográfica
- Visualização da validade ou data de cancelamento
- Impressão de segurança (por exemplo, microimpressão)
- Artefatos de segurança ótica inseridos, como hologramas e artefatos óticamente variáveis ou tintas ultravioleta.
- Laminação de segurança sobre a informação impressa.
- Correção da construção.
- Fotografia do portador do documento.
- Informação em meio de leitura mecânica (por exemplo, código de barras ou caracteres óticos).

Autenticação do dispositivo da Identidade

Para assegurar que o artefato eletrônico usado no ID que é apresentado é autorizado e não é fraudulento, o artefato é autenticado eletronicamente tipicamente através do uso de chaves secretas simétricas compartilhadas, chaves público/privadas assimétricas ou uma senha de autenticação (OTP). A verificação eletrônica é conseguida utilizando um dispositivo que “lê” o ID. O processo de autenticação pode ser estabelecido entre o ID e o leitor ou pode requerer que o leitor se comunique com um sistema de hospedagem ou um servidor de autenticação.

Autenticação pelo uso de chave secreta simétrica compartilhada. Para autenticar um ID usando uma chave secreta simétrica compartilhada, tanto o dispositivo de ID como o leitor devem conhecer a chave secreta comum (compartilhada). O leitor apresenta ao dispositivo uma senha que deve estar codificada de alguma maneira com a chave secreta compartilhada. O resultado é enviado do dispositivo de ID para o leitor e verificado contra um cálculo independente realizado pelo interpelador. Se o resultado combinar, o ID é considerado autêntico. Uma variação é acrescentar códigos de autenticação de mensagem (MACs) a todas as mensagens; estes proporcionam a mais forte autenticação quando o MAC é computado em tempo real com base na charada do leitor.

Autenticação pelo uso de chaves público/privada assimétricas. Este mecanismo se fundamenta no artefato de ID gerar um par de chaves público/privada assimétricas, com a parte pública acessível a todas as partes que necessitam verificar a autenticidade do artefato. Quando um leitor deseja testar o ID ele pode apresentar uma charada para que o artefato assine digitalmente usando sua chave privada. Quando o artefato retorna a informação, o leitor pode verificar a assinatura digital do artefato utilizando sua chave pública. Uma variação desta técnica requer que o ID assine um corpo de texto ou informação que é transmitido para equipamentos externos em tempo real.

Senha de uso único (OTP). Senhas de uso único servem como credenciais de autenticação dinâmicas que tem vida útil muito limitada para prevenir ataques a bases de senhas comuns.

A autenticação baseada em OTP ocorre de duas maneiras: ou síncrona, onde tanto o artefato que está sendo autenticado e o servidor de autenticação agem de forma congruente, ou assíncrona, ou charada-resposta, onde a informação é trocada de forma segura entre o servidor de autenticação e o artefato.

Autenticação de Leitor

Chaves secretas simétricas compartilhadas também podem ser usadas para autenticar o leitor do ID. Neste caso, o ID emite uma charada para o leitor e verifica o resultado com um valor calculado internamente. Obtendo uma resposta satisfatória, O artefato de ID não vai divulgar nenhum conteúdo de suas credenciais. Esta técnica é usada para prevenir leitores falsificados de serem capazes de se apropriar da informação da credencial que poderia ser usada na confecção de IDs falsificados.

Autenticação da credencial ID

As credenciais digitais armazenadas no cartão ID podem ser autenticadas usando uma assinatura digital do emitente ou uma mensagem de autenticação codificada. Neste caso, a autenticação da credencial é baseada em informação estática. Outras técnicas precisam ser usadas para assegurar que a informação não está sendo clonada ou comprometida de outra forma, ou que não está apresentada num ataque de resposta. Uma complicação adicional é que o leitor também deve ser capaz de verificar a data de expiração da credencial.

Autenticação do portador do ID

A pessoa portadora de um cartão ID pode ser autenticada de duas maneiras, checando-se:

- O que o usuário sabe (por exemplo, um PIN ou senha) e/ou
- O que o usuário é (por exemplo, um biométrico).

A entrada de um PIN ou senha indica ao dispositivo eletrônico no ID que o usuário está presente. Isso permite que o dispositivo libere a credencial de identidade do portador do ID, ou permita o seu uso.

Para verificar “o que o usuário é”, ou a foto no cartão ID é comparada à face do portador do ID ou faz-se uma comparação biométrica automatizada. Sistemas ID baseados em biométricos capturam uma imagem biométrica “ao vivo” (por exemplo, uma impressão digital ou um scan da geometria da mão) e a compara à imagem biométrica capturada quando o indivíduo foi registrado no sistema. Este tipo de comparação biométrica um-a-um verifica que o portador do ID é de fato a mesma pessoa registrada no sistema ID e é a pessoa correta que pode usar o ID. Biométricos também podem proteger o acesso a credenciais num ID.

O papel do cartão smart na cadeia de confiança

A tecnologia cartão smart pode fortificar muitos dos elos da cadeia de confiança num sistema ID seguro. Cartões smart atuam como o cartão ID do indivíduo e permitem acesso seguro a informações e serviços em sistemas projetados para atuar tanto *online* como *offline*. Com a capacidade de armazenar, proteger e modificar informação escrita no dispositivo eletrônico do cartão (ou seja, o chip), cartões smart oferecem uma flexibilidade que ainda não foi superada e opções para a troca e transferência de informações, ao mesmo tempo em que provêm a habilidade única de características de proteção de privacidade.

Suporte para identidade física e digital. Os cartões smart possuem a capacidade única de facilmente combinar identificação e autenticação tanto no mundo físico como no digital. Isso pode gerar economia significativa, pois o cartão ID baseado no cartão smart pode ser usado não somente para permitir acesso físico aos serviços mas também permitir aos indivíduos que se utilizem de serviços *online* como o pagamento de taxas, solicitação de documentos (por exemplo, uma certidão de nascimento) e o acesso a redes seguras.

Acesso à informação autenticada e autorizada. A informação necessária para identificar um indivíduo depende tipicamente do papel do mesmo na situação. Por exemplo, quando se compra cigarros, a única informação

necessária é a idade do comprador. Neste caso, se ele possui carteira de habilitação ou não, é irrelevante.

A habilidade do cartão smart de processar informação e reagir com seu ambiente lhe assegura a vantagem única de prover acesso autenticado à informação. O cartão smart é capaz de liberar apenas a informação requerida, quando ela é requerida. Diferentemente de outras formas de identificação (como uma passiva carteira de motorista impressa), um cartão smart não expõe toda a informação pessoal do indivíduo (inclusive possível informação não pertinente) cada vez que é apresentado.

Segurança do cartão ID forte. Quando comparado a outros cartões ID resistentes à manipulação, os cartões smart representam a melhor relação custo-benefício. Quando usado com outras tecnologias como chave pública criptográfica e dados biométricos, os cartões smart são praticamente impossíveis de serem duplicados ou forjados e a informação armazenada no chip não pode ser modificada sem a devida autorização (senha, autenticação biométrica ou chave criptográfica de acesso).

Cartões smart também podem auxiliar a deter a falsificação e tentativas de furto. Os cartões smart incluem uma variedade de recursos de hardware e software que identificam e reagem às tentativas de penetração e ajudam a deter possíveis ataques. Onde os cartões ID smart forem usados para verificação manual de identidade, recursos de segurança visual podem ser acrescentados ao corpo do cartão smart.

Segurança da credencial ID. Proteger a privacidade, autenticidade e integridade da informação codificada num ID tal como credenciais é um dos requisitos básicos de um sistema ID seguro. Informação sensível é normalmente criptografada, tanto no cartão ID smart como durante a comunicação com o leitor externo. Assinaturas digitais podem ser usadas para assegurar a integridade da informação, com a necessidade de assinaturas múltiplas no caso de informação inserida por diferentes autoridades. A fim de assegurar a privacidade, as aplicações e informações no cartão devem ser projetadas de modo a não permitir que essas informações sejam compartilhadas de alguma forma.

Autenticação dos componentes do sistema. Para segurança e privacidade mais robustas, o sistema de ID seguro pode exigir que componentes do sistema autenticuem a legitimidade de outros componentes durante o processo de verificação de identidade. O cartão ID smart pode verificar que o leitor de cartão é autêntico, e este por sua vez pode autenticar o cartão ID smart. O cartão ID smart também pode assegurar que o sistema que está solicitando a informação está devidamente autorizado a obtê-la.

Suporte do cartão smart para requisitos de privacidade. O uso de cartões smart reforça a capacidade do sistema de proteger a privacidade individual². Diferentemente de outras tecnologias de identificação, os cartões smart podem implementar um firewall pessoal para o indivíduo, liberando apenas a informação solicitada quando for solicitada. A habilidade única do cartão de verificar a autoridade do requerente da informação e forte segurança do cartão e da informação fazem com que ele seja um excelente depositário da informação pessoal de seu proprietário. Por permitir acesso autorizado e autenticado apenas à informação necessária para uma transação, um sistema de ID baseado em cartão smart pode proteger a privacidade individual ao

² Para informação adicional em como os cartões smart melhoram a privacidade num sistema ID, veja o “papel branco” da Smart Card Alliance intitulado “Privacy and Secure Identification Systems: The Role of Smart Cards as a Privacy-Enabling Technology,” que se encontra disponível no endereço www.smartcardalliance.org.

mesmo tempo em que assegura que o indivíduo está propriamente identificado.

Cartão smart e biométricos. Sistemas de ID seguros que requerem um alto grau de segurança e privacidade estão implementado as tecnologias smart e biométrica concomitantemente. A combinação de cartão smart e biométricos é uma tendência natural ao permitir dois ou mais fatores de autenticação. O cartão smart é o meio lógico para armazenamento da informação biométrica. Durante o processo de registro a imagem biométrica pode ser armazenada no chip para posterior verificação. Apenas o usuário autorizado com um biométrico compatível com o dado armazenado receberá acesso e privilégios no sistema.

Resumo da cadeia de confiança

Qualquer sistema ID deve definir os objetivos de segurança apropriados e seus atributos na política de segurança. Esta política deve identificar o grau de segurança que é apropriado e comedido ao valor dos recursos a serem protegidos. Ao desenvolver uma política de segurança, deve ser dada atenção cuidadosa a cada elo na cadeia de confiança ao usar o cartão ID e credencial. Se o sistema irá se basear em identificação manual ou visual, atenção adequada deve ser dada ao treinamento de quem deverá tomar as decisões sobre a autenticidade do cartão ID e das credenciais, e políticas devem ser seguidas no caso de falhas ao seguir os procedimentos.

Uma cadeia de confiança robusta e completa para um cartão ID e credenciais é mandatória para um sistema ID seguro. Com o advento dos cartões smart, artefatos eletrônicos que armazenam credenciais ID e verificação biométrica, o nível de confiabilidade de uma credencial apresentada aumenta consideravelmente. O elemento eletrônico (ou seja, o chip num passaporte eletrônico ou cartão ID smart) é o agente de segurança portátil do emissor do documento e um elo vital na cadeia de confiança de qualquer sistema sério de ID seguro.

Conclusões

Sistemas de identificação são necessários tanto em organizações públicas como em privadas. Os sistemas ID podem operar completamente dentro de uma organização (o ID de um empregado), cobrir organizações múltiplas (dentro de organismos governamentais ou entre empresas e seus clientes), ou se estender para a população em geral. Dada a complexidade do problema de verificação de identidade, o número de partes envolvidas e o número de escolhas no projeto do sistema de ID, não é de se surpreender que muitos sistemas de ID hoje sejam vulneráveis.

Para responder a essa vulnerabilidade e implementar um sistema ID seguro, as organizações devem definir uma cadeia de confiança que abranja todos os componentes e processos do sistema ID seguro. A cadeia de confiança começa com a definição do modelo confiável, das políticas de segurança, dos acordos comerciais entre as organizações envolvidas no sistema ID seguro e incluem todos os componentes do sistema ID – desde os processos e documentos usados na verificação inicial da identidade de um indivíduo que é registrado no sistema ID até a utilização do sistema no gerenciamento do sistema ID.

Cartões smart são um elo vital na cadeia de confiança de um sistema ID seguro. Eles servem como agente de confiança do emissor e empregam

habilidades únicas para verificar segura e acuradamente a identidade do portador do cartão, autenticar sua credencial ID e passar a credencial para o sistema ID.

Como discutido neste informe, sistemas ID baseados no cartão smart oferecem benefícios significativos para indivíduos, empresas e governos. Indivíduos usando cartões smart gozam grande satisfação por contarem com rapidez, conveniência e segurança no acesso a informações e serviços. A eficiência, consolidação de programas e características de segurança fornecidas pelo uso de cartões ID smart permite aos governos e organizações enriquecer a segurança ao mesmo tempo em que melhoram os serviços e reduzem os custos. Cartões smart fornecem uma plataforma de segurança ótima para um sistema de ID seguro que pode atender aos requisitos de governos e empresas quanto à verificação de identificação segura e acurada.