



Acesso Lógico Seguro: A função dos cartões inteligentes na autenticação confiável

Informe da Smart Card Alliance

Data de publicação: Outubro de 2004

Número da publicação: ID-04002

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

Sobre a Smart Card Alliance Latinoamérica (SCALA)

A Smart Card Alliance Latino América (SCALA) 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 © 2004 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.

Membros da Smart Card Alliance: Os membros podem acessar a todos os informes da Smart Card Alliance sem custo algum. Favor consultar à seção de login dos membros do sitio web da Smart Card Alliance, para acessar a informação com respeito aos direitos de reprodução e distribuição dos membros.

Agências governamentais: Os empregados governamentais podem solicitar copias grátis deste informe contatando info@smartcardalliance.org ou afiliando-se a Smart Card Alliance como um membro governamental.

Índice

RESUMO EXECUTIVO	5
INTRODUÇÃO	8
VISÃO GERAL DO ACESSO LÓGICO	10
MÉTODOS ATUAIS PARA ACESSAR A REDES DE COMPUTADORES	10
PROGRAMAS DE INTERFACE OU "DRIVERS" PARA SISTEMAS DE ACESSO LÓGICO MAIS FORTES	11
<i>Custos administrativos:</i>	11
<i>Riscos de Seguridade</i>	11
<i>Riscos de incumprimento das leis e regulamentos</i>	12
<i>Roubo de privacidade e identidade</i>	12
<i>Evolução tecnológica e Migração</i>	13
O PAPEL DOS CARTÕES INTELIGENTES	13
VISÃO GERAL DAS TECNOLOGÍAS DE AUTENTICAÇÃO.....	15
CONTRA-SENHAS	15
<i>Contra-senhas não encriptadas ou "Cleartext Passwords"</i>	16
<i>Conversão de Contra-senhas ou "Password Conversions"</i>	17
<i>Contra-senhas de Uso Único ou "One-time Passwords" (OTPs)</i>	18
FATORES BIOMÉTRICOS.....	20
CRIPTOGRAFIA DE CHAVE PÚBLICA	21
FICHAS SENSÍVEIS OU SOFT TOKENS	22
TECNOLOGIA DE CARTÕES INTELIGENTES.....	22
RESUMO	24
FATORES IMPORTANTES A CONSIDERAR PARA IMPLEMENTAR UMA AUTENTICAÇÃO MAIS PODEROSA DE ACESSO LÓGICO.....	25
AMBIENTE CORPORATIVO	25
TRANSFORMAÇÃO DO NEGÓCIO E RE-ESTRUTURAÇÃO DO PROCESSO	26
REDUÇÃO DE CUSTOS E RETORNO DA INVERSÃO.....	26
SEGURANÇA E PRIVACIDADE	27
GERÊNCIA, USO E CAPACITAÇÃO	28
BENEFÍCIOS QUE OFERECE A TECNOLOGIA DE CARTÕES INTELIGENTES PARA O ACCESSO LÓGICO.....	29
AUTENTICAÇÃO FORTE	29
SEGURANÇA INCORPORADA AO SISTEMA	30
AUMENTO DA SEGURANÇA E CONVENIÊNCIA PARA USUÁRIOS.....	31
PROTEÇÃO AUMENTADA CONTRA FRAUDES DE IDENTIDADE.....	32
COBERTURA DE APLICAÇÕES BASEADAS EM ESTÁNDARES	32
FÁCIL DE INTEGRAR.....	34
FÁCIL DE DISTRIBUIR	35
FUNÇÃO UNIVERSAL.....	35
CARTÕES INTELIGENTES USADOS COMO CRACHÁS DE IDENTIFICAÇÃO INTELIGENTE: EXEMPLO DE ESCENÁRIO.....	37
AS VANTAGENS SOBRE OUTRAS ALTERNATIVAS DE ACESSO LÓGICO	38
OS CARTÕES INTELIGENTES E A INFRA-ESTRUTURA IT	41
MICROSOFT WINDOWS	41
<i>Cartões Inteligentes e as Comunicações dos leitores</i>	41
<i>Autenticação do usuário</i>	43
<i>Serviço de Web e E-mail</i>	43
<i>Sistema de Encriptação de Arquivo</i>	44
<i>Suporte Oferecido por Diferentes Versões de Windows</i>	44

LINUX	44
<i>Cartões Inteligentes e as Comunicações dos leitores</i>	45
O USO DE CARTÕES INTELIGENTES PARA MÚLTIPLAS APLICAÇÕES	48
O USO DE MÚLTIPLAS APLICAÇÕES.....	48
<i>Controle de acesso físico</i>	48
<i>Pagos</i>	49
<i>Gerência e Armazenamento de Dados Seguros</i>	50
<i>Acesso a Rede Inalámbrica</i>	51
INSTALAÇÃO DA APLICAÇÃO	51
EXEMPLOS DE MÚLTIPLAS FUNÇÕES	51
PROPOSTA DE NEGÓCIOS ONDE SE USAM CARTÕES INTELIGENTES E ACESSO LÓGICO	53
BENEFÍCIOS INTANGÍVEIS	53
<i>Regulatory Compliance</i>	53
<i>Posicionamento Estratégico</i>	53
BENEFÍCIOS TANGÍVEIS.....	54
<i>Uso Administrativo Simplificado para el Usuario</i>	54
<i>Eliminação das Fichas OTP</i>	54
<i>Redução da Infra-estrutura global</i>	54
<i>Aumento da Produtividade</i>	55
INVESTIMENTOS	55
CONCLUSÕES	57
REFERÊNCIAS E FONTES.....	58
RECONHECIMENTOS	60
APPENDIX A: DEFINITION OF TERMS AND ACRONYMS.....	62

Resumo Executivo

A Pobre Segurança que Provêm as Contra-senhas para o Acesso Lógico a Redes de Recursos

Organizações de todos os tamanhos e de todas as indústrias estão ansiosas por melhorar o processo de identificação de usuários dos seus sistemas de redes. Com o aumento no uso de redes alámbricas e inalámbricas para aceder a recursos de informação e, com o aumento dos roubos de identidade e ataques a redes corporativas, a autenticação de usuários baseada em contra-senhas de acesso converteu-se em um risco significativo. As contra-senhas de acesso são comumente controladas pelo proprietário destas, quem pode usar uma contra-senha fácil de adivinhar, compartí-la com outros, escrevê-la, ou usar a mesma para aceder a vários sistemas. Ao mesmo tempo, o fato de armazenar informação das contra-senhas de acesso em redes corporativas lhe agrega ainda mais vulnerabilidade, a atacantes que ganham acesso às redes.

O gerenciamento de contra-senhas de acesso representa um custo significativo para as organizações. As estadísticas da indústria mostram que um 30% a 50% dos recursos de suporte técnico dos sistemas de informação (IT) são consumidos pela contínua troca das contra-senhas de acesso.

Tanto as agências governamentais como as empresas estão substituindo simples contra-senhas de acesso por outros sistemas universais de autenticação que fortalecem a segurança da informação, respondem ao mercado e as condições regulatorias e diminuem os custos de suporte técnico.

Uma variedade de tecnologias pode autenticar aos usuários para conseguir acesso lógico

Entre as tecnologias usadas para autenticar a identidade dos indivíduos que utilizam um acesso lógico incluem contra-senhas de acesso (com um número de variações – não encriptadas ou “cleartext”, encriptadas e de uso único), chaves de acesso simétricas, chaves de acesso público/ privado simétricas e informação biométrica. Os indivíduos comumente provam a sua identidade usando um único fator de autenticação. Entretanto, um sistema de autenticação de identidade mais sólido requer o uso de dois ou três fatores, tais como: algo que você tem (um objeto ou um amuleto seu), algo que você sabe, informação que só você sabe), ou algo que você é (uma qualidade física única ou conduta que diferencia você dos demais).

Os cartões inteligentes abarcam todas as tecnologias de autenticação, arquivos de contra-senhas de acesso, infra-estrutura de certificados públicos contra-senhas, base de dados de acesso único e plantilhas biométricas de imagem, assim como, chaves de acesso assimétricas emparelhadas. Um cartão inteligente combinado com uma ou mais tecnologias provê, de forma significativa e universal, uma segurança mais ponderosa na autenticação do acesso lógico. A tecnologia de cartões inteligente também provê flexibilidade para incluir todos os fatores de autenticação em um único cartão, aumentando todo o processo de segurança e autenticação.

A Tecnologia de Cartão Inteligente Prove Significativas Vantagens para Implementar uma Autenticação mais forte.

A tecnologia de cartões inteligentes fortalece significativamente a segurança, protegendo a credencial eletrônica usada para autenticar a um indivíduo e utilizando um acesso lógico como dispositivo físico. Tomando em conta que a credencial é armazenada permanentemente no cartão, esta nunca está disponível no programa ou na rede, para que um usuário não autorizado possa roubá-la. Os cartões Inteligentes constroem uma espécie de proteção para o dispositivo físico por meio de um suporte de resistência e técnicas ativas de segurança para a encriptação das comunicações.

Os cartões Inteligentes estão transformando-se no método preferido de acesso lógico, não somente por serem mais seguros, senão, também, pela sua facilidade de uso, ampla cobertura de aplicação, sua facilidade de integração com a infra-estrutura IT e sua funcionalidade universal. Os sistemas operativos Microsoft® Windows® e Unix® oferecem um significativo nível de cobertura de apoio relacionada ao cartão inteligente, já seja, incorporado ou como pacotes adicionais de "softwares" comerciais. Os cartões inteligentes baseados em acesso lógico permitem às empresas emitir um só cartão de identificação que abarca o acesso lógico, o acesso físico e mantém seguro o armazenamento da informação, assim como a outras aplicações. Ao combinar múltiplas aplicações em um único cartão de identificação, as organizações podem reduzir custos, aumentar a conveniência do usuário final e prover melhor segurança para as diferentes funções.

A tecnologia de cartão inteligente provê às organizações um acesso lógico rentável. Os cartões Inteligentes representam uma oportunidade de negócios positiva para implementar qualquer tecnologia de autenticação, aumentar a produtividade do usuário, reduzir custos nas contra-senhas de acesso administrativo, diminuir o risco de exposição e alinhar os processos de negócios. Tudo isto contribui a um significativo e positivo retorno da inversão.

Com respeito a este informe

Este informe foi desenvolvido pela Smart Card Alliance com o objetivo de prover informação sobre as tecnologias de autenticação usadas para o acesso lógico, e para descrever como os cartões inteligentes fortalecem os processos de autenticação.

Diseñado como uma revisão educativa para a toma de decisões, este informe provê respostas para as perguntas normalmente feitas com respeito ao uso dos cartões inteligentes para o acesso lógico, tais como:

- Por que as organizações buscam formas mais poderosas de autenticação do acesso lógico às redes de recursos?
- Que tecnologias de autenticação estão disponíveis e o que têm em comum?
- Como são os cartões Inteligentes usados para a autenticação e quais benefícios brindam a uma organização?
- Como os cartões inteligentes são integrados na estrutura IT?
- Qual são os exemplos de negócio onde se utilizam os cartões Inteligentes para acesso lógico?

-
- Em que outras aplicações se pode usar a tecnologia de cartões inteligentes, e como um cartão universal beneficia a organização?

O informe inclui perfis de organizações que estão usando cartões de identificação inteligentes para o acesso lógico, como por exemplo: Boeing, Microsoft, Rabobank, Shell, Sun Microsystems, U.S. Department of Defense e o U.S. Department of State.

Introdução

Nos centros de trabalho de hoje, assegurar o acesso lógico é uma preocupação crítica. A Internet facilitou a colaboração efetiva entre sócios, clientes e provedores. Novas tecnologias permitem que os trabalhadores de campo possam comunicar-se fora dos perímetros de segurança tradicional, usando tecnologia inalámbrica ou, trabalhar, remotamente, sobre uma rede virtual privada (VPN). As crescentes eficiências operacionais motivam a um número cada vez maior de empresas e organizações de serviço (tais como, bancos, companhias de saúde e seguros) para evoluir a uma rede de negócios composta por portais corporativos, servidores de aplicação e recursos Web protegidos. O crescente aumento na incidência de roubos de identidade e com o advenimento de novas regulações e legislações, tais como a Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley Act, e a Gramm-Leach-Bliley Act, também contribuíram a um ambiente no qual manter seguro o acesso lógico é extremamente importante. Por todas estas razões, organizações que administram identidades de usuários, políticas de autenticação e privilégios de usuários enfrentam o reto de impedir que os intrusos tenham acesso à informação do proprietário.

A infra-estrutura do acesso lógico baseada no uso de contra-senhas, falha na resolução destas novas ameaças: os novos modelos de negócios e o complexo crescimento ao acesso dos recursos de rede. As contra-senhas são caras de administrar (um estimado de 30 % ao 50 % dos custos de suporte técnico são atribuíveis ao reajuste das contra-senhas de acesso) e podem ser quebrantadas utilizando uma ampla variedade de ferramentas. As preocupações emergentes, como resultado do uso de sistemas baseados no acesso, e a conveniência agregada que oferecem os cartões inteligentes, podem ser as duas principais razões pelas quais as organizações estão emigrando ao uso de sistemas de acesso lógico baseados em cartões inteligentes. Segundo um sondeio realizado pela Frost & Sullivan, o 39% das companhias pertencentes ao Grupo Fortuna 500, planejam utilizar cartões inteligentes nos próximos três anos e, o 63% das 500 companhias pertencentes ao Grupo Fortuna 500 já investigaram ou estão investigando a implementação da tecnologia de cartões inteligentes em suas redes de segurança.

A tecnologia de cartões inteligentes está disponível em diversas formas: um cartão plástico, um dispositivo periférico externo (USB), ou um cartão SIM (Subscriber Identification Module) em um telefone celular. Cada uma delas têm um micro-circuito semi-condutor que pode ter uma memória micro-controladora cripto-coprocessadora, um sistema operativo e um programa de aplicação. A capacidade computacional dos cartões inteligentes iguala a capacidade computacional da primeira computadora pessoal (PC); os cartões Inteligentes possuem todas as características de um computador, exceto um teclado e um monitor. O micro-circuito dos cartões Inteligentes estão decontra-senhados para resistir a ataques utilizando diversas medidas anti-criptação, fazendo inverossímil que os dados armazenados no cartão inteligente sejam expostos, roubados, modificados, ou destruídos. A capacidade única dos cartões inteligentes de proporcionar armazenagem segura de dados e as funções de suporte criptográficas sofisticadas, o convertem na melhor opção para autenticar a indivíduos que utilizam um acesso lógico.

A tecnologia de cartões Inteligentes evolucionou durante os últimos 20 anos proporcionando como resultado: capacidades melhoradas de

armazenagem, processamento e segurança, um programa de administração do cartão inteligente, tecnologias sem contato e a integração de diversas funções em um único cartão de identificação. Os cartões Inteligentes podem incorporar inúmeras aplicações utilizadas pelas organizações que incluem acesso mediante Windows, administração de contra-senhas de acesso, contra-senhas de acesso de uso único (One Time Passwords OTP), autenticação VPN, correio eletrônico com dados encriptados, assinaturas eletrônicas, acesso único a empresa, acesso a redes inalámbricas de forma segura, autenticação biométrica, pagos de cafeteria, armazenamento de informação pessoal, a acesso baseado em funções, acesso físico seguro, assim como a lealdade do cliente. Hoje em dia, os cartões Inteligentes são essenciais para o sistema de administração de identidade de uma organização, cubrindo ponderosa autenticação requerida para validar os recursos individuais do acesso às redes e provendo um importante primeiro passo para o bloqueio de intrusos.

O trabalho de estandarização levado a cabo pela Global Platform e o Government Smart Card Interoperability Specification (GSC-IS) capacita aos que emitem cartões, combinar soluções de múltiplos recursos, assegurando, por tanto, inter-operabilidade a larga escala e reduzindo os custos de propriedade ao prover um mercado aberto. Devido às significativas inversões, ainda se requer integrar novos sistemas de autenticação que dirijam a uma infra-estrutura heredada e, compromisso em curso por parte dos altos executivos, uma dedicada administração do projecto, para fazer exitoso o novo sistema de administração de identidades e sua implementação. As organizações que adotem o uso de cartões inteligentes para o acesso lógico vêm um sólido retorno das inversões e significativos benefícios, incluindo melhorias na conveniência e segurança, maior responsabilidade, melhores decisões de seguridade, regulações conformes, eficiências operacionais e novas oportunidades de negócios.

Este informe explica os conceitos necessários para entender que as tecnologias de autenticação são usadas para o acesso lógico, e como os cartões Inteligentes podem ser usados para fazer o acesso lógico mais seguro. Muitas organizações utilizaram os cartões Inteligentes exitosamente em seus sistemas de acesso lógico, vemos os perfis de sete delas -Boeing, Microsoft, Rabobank, Shell, Sun Microsystems, U.S. Department of Defense and U.S. Department of State – estão incluídos no apêndice deste informe.

Visão Geral do Acesso Lógico

O Acesso lógico é o processo pelo qual se permite aos indivíduos usar os sistemas computacionais (os quais podem incluir outros dispositivos digitais, tais como, PDAs e celulares) e a rede na qual esses sistemas estão/são unidos/conectados (tais como, redes de áreas de uso corporativo e redes de área de uso aberto, redes e telecomunicações, intranets/extranets, e redes inalámbricas). O objetivo do acesso lógico seguro é assegurar que estes dispositivos e redes, e os serviços que eles provêm, estejam disponíveis somente para aqueles indivíduos autorizados para usá-las. Por direito se baseia normalmente em algum tipo de relação predeterminada entre o proprietário do sistema ou a rede e o usuário, ou algum outro tipo de relação estreita.

O sistema que abarca a prestação deste tipo de serviços representa uma significativa inversão, que, de fato, pode representar o maior ativo que tem a organização. Estes ativos requerem proteção para evitar o seu uso por indivíduos ou organizações não autorizados, os quais pudessem diminuir ou destruir seu valor. Por tanto, controlar o acesso a esses ativos é de suprema importância virtualmente para todas as organizações que dependem dos sistemas de tecnologia de informação (IT) para alcançar seus objetivos.

Métodos Atuais para Acessar a Redes de Computadores

O método mais amplamente implementado para controlar o acesso lógico é o de identificar o usuário utilizando uma combinação de contra-senha e identificação. Os usuários provêm a sua contra-senha, normalmente o nome do usuário ou um segredo que somente o usuário conhece. Um simples buscador de dados programado determina que a contra-senha está ligada ao usuário, autenticando a identidade do usuário; a autenticação pelo geral asigna uma identificação única de acesso, e combinando a identificação única do usuário com a sua contra-senha, o sistema determina os níveis de acesso para esse usuário baseando-se nessa identificação única do usuário.

Com o tempo, entretanto, este tipo de autenticação provou ser frágil e ineficiente. A identificação de usuários e contra-senhas de acesso podem peligrar facilmente por meio de conhecidas técnicas. Quando esta classe de informação é obtida por elementos criminais, esta pode ser usada para alcançar uma entrada ilegal e não autorizada a uma rede. Os resultados dos controles de acesso comprometidos podem ser desastrosos para o proprietário da rede e para o usuário cuja rede ou sistema de identidade é roubado. Adicionalmente, as identidades do usuário são, pelo geral, administradas por aplicativos, criando ineficiências operacionais na medida em que esses sistemas e aplicações em uma organização crescem e introduzem vulnerabilidade à seguridade, tornando-o cada vez mais difícil controlar as políticas de uso destas identidades.

Afortunadamente, existem novas tecnologias disponíveis que podem fortalecer os processos de autenticação cubrindo controles de acesso e provendo níveis mais altos de garantia, assegurando que os usuários são os que eles dizem ser e que as credenciais de identidade apresentadas são válidas. Estas tecnologias, descritas nas seguintes seções, geralmente agregam técnicas de encriptado, informação biométrica de algum tipo e/ou a posse de crachás ou credenciais para melhorar a efetividade dos sistemas de controle de acesso. A diferença do uso de somente um elemento (por exemplo, a combinação de acesso de identificação de usuário e contra-senha), a sólida autenticação requer o uso de dois ou três fatores para validar a identidade.

Os fatores poderiam incluir alguma combinação de algo que você sabe (uma contra-senha ou o número de identificação pessoal que só você conhece), algo que você tem (um objeto físico que possua) e algo que você é (uma característica física ou comportamento que te distinga de outros indivíduos).

O uso de poderosas tecnologias de autenticação e múltiplos fatores de autenticação diminuem a perda potencial da informação devido ao acesso desautorizado aos ativos da rede.

Programas de Interface ou “Drivers” para Sistemas de Acesso Lógico Mais Fortes

A segurança em risco não é a única razão pela qual se investigam melhoras nas técnicas de controle do acesso lógico. Outras desvantagens no uso combinado de contra-senha e identificação incluem os altos custos administrativos, a capacidade inadequada de administrar diversos riscos e a incapacidade para nivelar a segurança adicional com a qual se constroem os sistemas computacionais e suas aplicações.

Custos administrativos:

Na medida em que os usuários acedem a um número cada vez maior de serviços de rede, cada um requerindo uma identificação e contra-senha independente, a habilidade dos usuários para administrar e lembrar informação de acesso requerida se reduz. Como resultado, os usuários têm que escrever a informação, o qual a faz vulnerável, ou comunicam a seus administradores de rede. Os administradores de rede pelo geral têm que lidar com as ligações de usuários que esqueceram a sua contra-senha, combinação de contra-senha e identificação.

Essas ligações de assistência usualmente são muito caras e estão em aumento, assim como o incremento dos serviços que se oferecem cada vez mais nas redes. Muitas fontes estimam que uma só ligação a um administrador para que reative uma contra-senha esquecida tem um custo aproximado de quarenta dólares. Os custos associados a gerência deste método de autenticação e controle de acesso estão levando aos administradores de redes a buscar soluções que sejam mais eficientes, assim como mais confiáveis.

Riscos de Segurança

Recentemente, multiplicaram-se os reportes de indivíduos não autorizados invadindo as redes computacionais para roubar informação com propósitos financeiros ou políticos.

No sector privado, o impacto destas falhas na segurança é medido em termos tanto de perdas financeiras como de perda da confiança do cliente. No âmbito governamental, o risco aumenta pelo efeito potencial sobre a segurança nacional e o impacto na credibilidade pública e na confiança das organizações governamentais mais importantes.

Na medida em que surgem mais intromissões, a habilidade para quantificar seu impacto negativo está aumentando. Instituições tanto no setor público como privado são mais capazes de analisar os custos e benefícios de investir em novas tecnologias para melhorar a segurança das redes, incluindo tecnologias para melhorar o controle do acesso e são capazes de justificá-lo com base nos sólidos retornos de inversão.

Riscos de incumprimento das leis e regulamentos

A raíz dos ataques terroristas do 11 de setembro, uma quantidade significativa de novas legislações tem sido aprovada, primariamente, encaminhadas a melhorar as redes de computadores e a sua administração pelo Governo Federal. As legislações adicionais promovem a adoção de sistemas que dirijam os serviços governamentais eletronicamente. Uma parte crítica destas iniciativas é o apoio a autenticação lógica de indivíduos tratando de aceder a esses serviços.

Como resultado disso, as redes e os mecanismos de segurança por meio dos quais os usuários têm acesso aos ativos controlados pelo governo colocaram-se entre as prioridades da agenda governamental. As políticas e guias de implementação definem os níveis de autenticação que são necessários, com base na sensibilidade da informação a aceder, e uma variedade de opções de tecnologias candidatas que têm sido identificadas, as quais variam entre identificações dos usuários e contra-senhas de acesso para infra-estrutura pública (PKI), biométrie e cartões inteligentes. Muitas agências governamentais dos Estados Unidos têm implementado programas para garantir que cartões de identificação inteligente apoiem as técnicas de autenticação mais eficientes, tanto para o acesso físico, quanto o lógico.

De fato, o governo já exige dos contratistas que cumpram com padrões específicos para tecnologias, políticas e práticas de segurança. A tendência do setor privado é a de adotar tecnologias e práticas implementadas pelo governo, não só como um exemplo de melhores práticas, mas também como um meio para mitigar qualquer risco legal que possa ocorrer por inconformidade. Os negócios também estão sujeitos a um número de novos requisitos de controle de acesso e auditoria, como resultado de novas leis e regulamentos, tais como: Gramm-Leach-Bliley Act, HIPAA, the Sarbanes-Oxley Act, e o USA Patriot Act.

Roubo de privacidade e identidade

Conforme a Federal Trade Commission, nos últimos 5 anos 27.3 milhões de americanos foram vítimas de roubos de identidade, tantos que quase \$48 bilhões de dólares foram utilizados por empresas e instituições financeiras com a finalidade de identificar os ladrões de identidade, e por sua parte as vítimas também abarcaram os gastos, ao redor de \$5 bilhões pelo mesmo motivo. Os ataques aos computadores dos consumidores mediante o fraudulento método denominado "phishing", vírus e ataques de "spyware", constituem novas formas para roubar os nomes de usuários e as contra-senhas.

Gartner reporta que mais de 1.4 milhão de americanos adultos têm sofrido fraude pelo roubo de identidade devido aos "phishing", os quais custaram aos bancos e aos emissores dos cartões de crédito ao redor de \$1.2 bilhão em perdas diretas no ano passado.

Na medida em que o roubo de identidade se transforma cada vez mais em um assunto de maior interesse (assim como é tema de discussão legislativa a nível estatal e nacional), o setor privado deverá estabelecer métodos mais estritos de controle nas bases de dados dos clientes e a informação pessoal que tal proteção se confiou as empresas. As companhias precisam controlar o acesso à informação sensível e garantir que a mesma seja somente acessível por aqueles com a apropriada autorização.

Evolução tecnológica e Migração

Devido a crescente demanda dos usuários de sistemas de informação que requerem melhores mecanismos de controle de acesso, os provedores de sistemas de informação estão oferecendo maior segurança a seus produtos com a finalidade de proporcionar apoio incorporado para as soluções modernas de autenticação. Por exemplo, o Windows vem agora com suporte para registro PKI e correio encriptado e firmado digitalmente. Mais e mais produtos de uma grande variedade de vendedores permitem o uso de tecnologia PKI, biométrica e tecnologia de cartões inteligentes para apoiar métodos mais poderosos de autenticação utilizando múltiplos fatores.

Na medida em que os sistemas computacionais são atualizados, com o tempo, o apoio tecnológico para conseguir medidas de autenticação mais poderosas, mediante o uso de múltiplas tecnologias, será mais fácil de ser obtido. Como resultado disso, se dará um crescente aumento no uso de técnicas mais poderosas de autenticação, maiores níveis de acesso de segurança e maior conveniência para o usuário.

O Papel dos Cartões Inteligentes

A tecnologia de cartões inteligentes pode desempenhar um papel importante dentro das soluções que provêm poderosas respostas de autenticação, rede de segurança melhorada e proteção as identidades e a privacidade dos indivíduos. Assim como um dispositivo criptográfico, o micro-circuito no coração do cartão inteligente pode apoiar um amplo número de usos e de tecnologias de segurança. Os cartões inteligentes oferecem armazenamento seguro de dados e apoiam poderosas medidas de autenticação requeridas para aceder à informação que incluem o seguinte:

- Suporte para chaves de aplicações de acesso simétricas e de PKI (exemplo, assinaturas digitais e encriptação de mensagens de correio eletrônico), geradores de chaves de acesso incorporados ao cartão, e proteção para a privacidade da chave de acesso do usuário.
- Armazenamento seguro para dados biométricos
- Armazenamento seguro da identidade do usuário e da sua senha de acesso
- Apoio para gerar contra-senhas de acesso de uso único
- Armazenamento seguro para chaves de acesso simétricas
- Apoio para outras aplicações como acessos físicos de controle ou transações financeiras

Na forma de cartão, a tecnologia de cartão inteligente pode, também, ser utilizada como um crachá de identificação universal, provendo um acesso visual de identificação, ao mesmo tempo que automatizado; igualmente, acessos autenticados físicos e lógicos.

Visão Geral das Tecnologias de Autenticação

Na história do Ali Babá e os Quarenta Ladrões, um tesouro roubado por 40 ladrões é escondido em uma caverna protegida por uma roca mágica. A única forma de entrar é dizendo a palavra secreta "Ábrete Sésamo". Não importa quem a diga, aquelas palavras ditas na forma correta, faziam que algo mágico acontecesse, movendo a roca e permitindo ao que a dizia entrar.

Esta mesma magia acontece quando alguém acessa a uma rede de computadores. A importância da autenticação não pode ser exagerada. Uma vez que uma pessoa é autenticada dentro da rede, os privilégios e direitos de acesso dela serão baseados baixo essa autenticação. O objetivo da autenticação é, por tanto, permitir acesso à rede a cada usuário que está autorizado, mantendo aqueles que não estão autorizados fora desta. A meta final de cada autenticação é negar o acesso a impostores sem causar problemas aos usuários válidos.

Vários enfoques estão dirigidos a alcançar essa tarefa vital, que dependerão da incorporação de um ou mais destes três fatores críticos para a autenticação, sendo eles os seguintes:

- Algum conhecimento que tem a pessoa, tal como uma contra-senha. Este fator esta relacionado com algo que você conhece. Esse fator esrtá relacionado, normalmente, com algo que você conhece.
- Alguma característica física, como uma impressão digital. O conhecimento que tem a pessoa, como uma contra-senha. Esse fator tem está relacionado, normalmente, com algo que você é".
- Algo que a pessoa possui, tal como uma chave, uma ficha, ou um cartão inteligente. Este fator é conhecido, normalmente, como "algo que você tem".

Cada aproximação individual e decontra-senhada de forma única com a finalidade de autenticar a cada usuário da maneira mais completa possível, sem criar uma grande incomodidade. Também, cada um têm uma debilidade potencial. Usados em combinação, se fortalece a autenticação reduzindo a possibilidade de que um impostor acesse.

Contra-senhas

A contra-senha é sem dúvidas a técnica de controle de acesso de maior uso. O usuário simplesmente prove um nome de usuário e contra-senha, suministra a informação e se lhe autoriza ou nega o acesso. Dentro do computador este método de autenticação compara o nome e a contra-senha do usuário para armazenar a informação. Uma resposta eletrônica garante ou nega o acesso baseado no resultado desta comparação. Proteger os nomes do usuário, as contra-senhas e a relação entre esses, é, portanto, crítico para controlar o acesso lógico com contra-senhas.

Existem muitas maneiras que o indivíduo não autorizado pode obter acesso as contra-senhas. Entre os mais comuns temos:

- **Engenharia Social (Social engineering)**, provavelmente a forma mais conhecida para obter acesso a um simples sistema. Por exemplo, indivíduos não autorizados usam razões aleatórias e lógicas para obter as contra-senhas de outras pessoas. Este risco é

Formatted: Bullets and Numbering

mais facilmente suavizado educando os usuários sobre a necessidade de uma maior e mais eficiente segurança.

- **Programas de abrir contra-senhas (Password cracking programs)** usam, já seja, a força bruta ou métodos de busca de dicionário para tentar decriptar contra-senhas protegidas.
- **Programas rastreadores (Sniffer programs)** monitorizam pacotes de informação que viajam dentro de rede. Se uma contra-senha não encriptada passa perto, rastreador captura e a usa, comprometendo a integridade do sistema. Entretanto, a efetividade das ferramentas de rastreio tem diminuído com a ampla adoção de “switches” de redes e roteadores, reduzindo grandemente a utilidade destas.
- **O conhecimento pessoal** sobre os usuários legítimos é usado para tratar de adivinhar suas contra-senhas.
- **Acesso das estações de trabalho dos empregados** uma pessoa pode se sentar no escritório de um empregado quando não tenha ninguém por perto e buscar contra-senhas que tenham sido escritas.
- **Olha e vê** a forma mais fácil de obter uma contra-senha é olhar as pessoas quando escrevem no teclado.

Com o objetivo de proteger a integridade da contra-senha, as políticas de segurança requerem que os usuários troquem as suas contra-senhas continuamente para impedir o acesso a suas contas através de métodos tais como encontrar contra-senhas escritas, ver as pessoas registrar sua contra-senha, mediante o uso de programas de rastreio do teclado ou adivinhando. Tais políticas de segurança de contra-senha são efetivas, mas podem chegar a ser bastante complicadas. Estas políticas alertam, normalmente, aos usuários a não reutilizarem as contra-senhas, obrigando-os a criar novas que sejam mais “difíceis de adivinhar” por outros, e fáceis de lembrar. A proteção da informação armazenada é também crítica para uma política de fortalecimento de medidas de segurança.

As contra-senhas podem ser implementadas em uma grande variedade de formas. De qualquer maneira, é recomendável o emprego de uma forte política de medidas de segurança. A política pode ser tão simples como pedir um número mínimo de letras, podem requerer a inclusão de letras maiúsculas e minúsculas, números e caracteres especiais.

Contra-senhas não encriptadas ou “Cleartext Passwords”

A forma mais elemental de armazenamento de contra-senhas é mediante o uso de contra-senhas não encriptadas (ou seja, não cifradas) onde as contra-senhas e os nomes dos usuários são armazenados em um fichário o qual é armazenado na rede. Este tipo de arquivo tem a seguinte aparência:

ALICEZ	MYDOGSPARKY
BOBY	HOME4HOLIDAYS
CAROLW	GETTHEJOBDONE

Esta aproximação é fácil de implementar. O desafio recai em proteger a informação contra o acesso ou a manipulação inadequada, enquanto que o

arquivo conserva a acessibilidade imediata para o processo de conexão. Enquanto que a aproximação é apropriado para certas situações, é extremamente vulnerável contra um ataque. Uma vez que os atacantes descobrem como a função da conexão trabalha e determinem que as contra-senhas estão mantidas no fichario, o acesso se simplifica grandemente. Uma vez dentro do sistema, o atacante lê simplesmente o arquivo e obtém os privilégios e o acesso da rede que estão registrados nas contas existentes dos usuários.

Conversão de Contra-senhas ou “Password Conversions”

Para diminuir a vulnerabilidade de armazenar contra-senhas não cifradas, as seguintes, são três técnicas enfocadas em converter a contra-senha não cifrada, introduzida pelo usuário, a outra forma de dado:

- Hashing
- Códigos de autenticação de mensagens ou “Message Authentication Codes” (MACs)
- Criptografia

As três técnicas sofrem, potencialmente, da mesma vulnerabilidade, todas dependem da capacidade de eleger as contra-senhas que são fáceis de lembrar (sem ter que anotá-las), mas são técnicas complexas para enfrentar os ataques; converter uma contra-senha protege a forma armazenada da contra-senha, de forma tal que elimina o acesso da base de dados da contra-senha. Entretanto, a contra-senha por si mesma segue sendo potencialmente vulnerável ante o “guessing” ou “sniffed replay” (onde o atacante intercepta informação que contém a contra-senha, extraindo ela desta informação).

“**Hashing**”. Conhecido às vezes como um resumo da mensagem, utiliza um algoritmo matemático unidirecional que cria um “resultado de longitude fixa” de uma mensagem de qualquer longitude.

O Hashing essencialmente cria uma impressão digital de uma mensagem, que neste caso é utilizada para proteger as contra-senhas. O Hashing muda uma contra-senha a um formato binário e a divide em blocos de códigos de um tamanho predeterminado. Cada bloco se processa, depois, através do algoritmo hash e se combina com o seguinte bloco que se processará, uma e outra vez, até terem sido processados todos os blocos.

O resultado, então, se converterá a texto ASCII. O Hashing é um método de confiança para converter contra-senhas porque o resultado de alimentar a mesma contra-senha no mesmo algoritmo é sempre igual. Entretanto, virtualmente nenhuma aproximação matemática ou lógica pode ter a contra-senha original com o resultado.

Os dois algoritmos de cálculo mais populares são MD5, que produz um hash de 128 bits procedentes de qualquer entrada, e o Secure Hash Algorithm (SHA) para ser usado com o Estándar de Assinatura Digital ou “Digital Signature Standard”, criada pelo National Institute of Standards and Technology (NIST) e a National Security Agency (NSA). O SHA-1 produz uns 160 bits de hash.

Uma contra-senha SHA-1 feita por este processo se veria assim:

USUÁRIO	CONTRA-SENHAS
AliceZ	c0f1ce0662f4a2f8d86613cf2e7ddc311fbcf3bd
BobY	6dc04707c1204dac18b73e5b388365deac43f70c
CarolW	2a70467b07eb3acfb90944c90e0261a5cb44649d

Códigos de Autenticação de Mensagens ou Message Authentication Codes (MAC). A proteção das contra-senhas que usam um código de autenticação de mensagens (MAC) depende de um processo, que primeiro “hashe” a contra-senha e depois agregue uma chave criptográfica simétrica. A segurança é realizada pelo fato que a “contra-senha hasheada” está cifrada. A localização verificada compara a contra-senha a um valor armazenado.

A contra-senha está preparada, normalmente, para ser transportada dentro do computador usado para conectar a rede. Assim como o hashing, os MACs protegem as contra-senhas somente depois que se registram.

Criptografia. As contra-senhas também podem ser protegidas usando a criptografia. Um algoritmo criptográfico residindo, geralmente, no computador do primeiro registro, encripta a contra-senha e a envia a uma localização onde residem os dados da contra-senha. A contra-senha é comparada aos dados armazenados e o resultado se envia de novo ao computador inicial de logeio.

Os algoritmos criptográficos simétricos se utilizam, normalmente, já que são rápidos e poderosos. A diferença do Hashing e do MAC, a a resposta alcançada varia referente a extensão da contra-senha.

Um arquivo de contra-senhas encriptadas se veria assim:

USUÁRIO	CONTRA-SENHAS
AliceZ	60135d5b849c2700dc60ffc2606fb947
BobY	0c0dd92d4bd8d8ca864441d23e066d8b
CarolW	7b94228224366ce3b2a049acaa0bd3c2

Contra-senhas de Uso Único ou “One-time Passwords” (OTPs)

As contra-senhas de uso único (OTPs) foram desenvolvidas para tratar com os problemas gerados por determinados usuários, contra-senhas fixas e com a administração de políticas de segurança para a administração de contra-senhas. As OTPs usam um algoritmo de tempo baseado em um gerador de números aleatórios que é único para cada usuário individual.

Cada vez que o usuário é autenticado pelo sistema, se utiliza uma contra-senha diferente, depois essa contra-senha caduca. A contra-senha é computada por um programa ao registrar-se ou por fichas do “hardware”

OTP, que possui o usuário e são coordenadas através de um sistema confiável.

Softwares baseados em OTPs. Os programas baseados em OTPs residem totalmente na rede e no computador central. Um dos programas baseados nos OTPs mais comum é o S/KEY®, que está livremente disponível em internet e se utilize, por exemplo, na seguinte discussão:

S/KEY utiliza uma combinação de uma contra-senha permanente de S/KEY que nunca se envia na rede e uma chave de acesso de uso único. Quando o usuário se conecta com a máquina remota, uma caixa de diálogo exibe uma chave de uso único e solicita uma contra-senha. A chave de uso único e a contra-senha permanente de S/KEY do usuário, são registradas em uma máquina local do cliente, usuário do S/KEY, que, então, gera uma contra-senha que permite a conexão. Cada vez que o usuário se conecta com a máquina remota, a chave de uso único muda, entretanto, a contra-senha permanente do S/KEY do usuário segue sendo igual.

Uma das vantagens alegadas para este enfoque é que os secretos não se guardam no Host do servidor. Entretanto, o servidor necessita guardar os OTPs utilizados recentemente para a autenticação. Por esta razão os programas baseados em OTPs são vulneráveis aos intrusos que obtêm os privilégios da raiz do servidor.

Fichas OTP. OTPs baseados em "Hardware" são gerados por uma ficha física ou por outros dispositivos que os usuários levam consigo. A geração de uma contra-senha se baseia em algoritmos de tempo ou algoritmos que respondem a mudanças(desafio-resposta). O algoritmo de tempo mais popular se incorpora no produto do RSA SecurID. Nesta posta em prática, o usuário leva um símbolo especial (token) que gera e exibe um número de seis dígitos que muda cada 60 segundos. Para ingressar em um sistema, o usuário incorpora um nome do usuário e utiliza o número de seis dígitos como contra-senha. Um servidor hospeda um programa que utiliza um relógio para coordenar com o dispositivo, mantendo uma base de dados com as contra-senhos e as respostas corretas às mudanças. Se o número é o esperado, o servidor aceita a contra-senha. Em um sistema de mudanças (sistema desafio-resposta), um desafio é dado pelo sistema hóspede, que então é utilizado pelo usuário para computar a resposta apropriada. A resposta pode ser computada com as fichas, um programa automático ou um software do usuário.

Técnicas de OTP alternativas estão disponíveis, incluindo os enfoques que usam um cartão inteligente ou um cartão inteligente baseado em fichas leitoras USB, tais como um dispositivo físico OTP.

Mecanismo de Acesso Único ao Sistema ou "Single Sign-On". É um mecanismo de autenticação que exige aos usuários do computador o acesso a um sistema (ou seja, apresentar uma contra-senha) uma só vez. Este mecanismo de acesso único lhes oferece o acesso a todas as aplicações e sistemas aos que estão autorizados a aceder. Os "Single sign-On" estão sendo postos em execução, normalmente, para reduzir o erro humano e a frustração do usuário. A aceitação desses mecanismos "Single-Sign-On" não tem sido universal, posto que estes reduzem, geralmente, somente, o número de contra-senhos requeridas ou, são muito complexas para integrá-las às aplicações. Devido a que os mecanismos "Single Sign-On" dependem das contra-senhos, estes mecanismos também sofrem das debilidades inerentes a todas as tecnologias de autenticação, ao menos que outras soluções de autenticação sejam implementadas.

Fatores Biométricos

Os métodos baseados em fatores biométricos abarcam a grupos de tecnologias provadas e de métodos automatizados que identificam e verificam a indivíduos baseando-se em suas características pessoais. Estes métodos aproximam uma característica em tempo real contra um expediente da característica que foi criada ao registrar-se ao sistema. As tecnologias biométricas principais incluem a impressão digital, a cara, a geometria da mão, o diafragma, a palma, a assinatura, a voz e a pele.

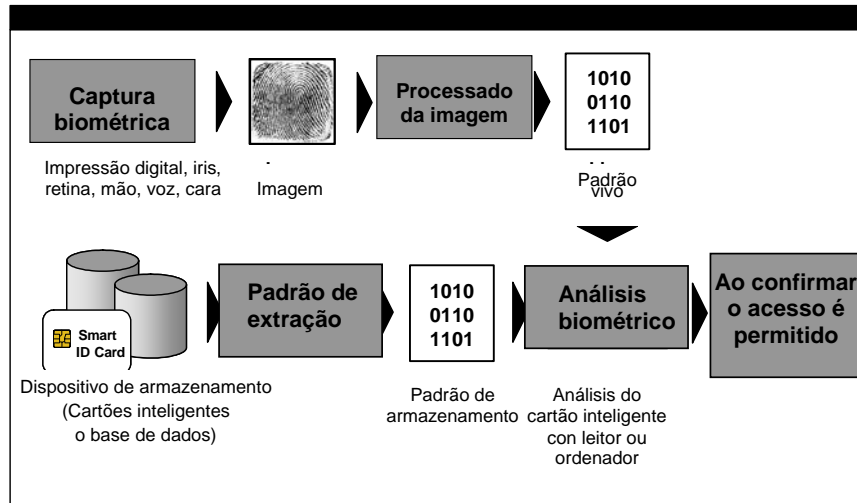
O processo de computado se realiza em três passos:

1. Uma imagem dos dados biométricos (exemplo: impressão digital) se captura.
2. A imagem se converte em uma planilha única.
3. Os algoritmos complexos comparam a planilha com o expediente armazenado.

As tecnologias biométricas estão sendo utilizadas como controle primário ou secundário para o acesso lógico. Em um panorama típico, os usuários incorporam um nome do usuário e colocam um dedo em um leitor (além de proporcionar uma contra-senha). Um servidor compara a planilha biométrica criada pelo leitor com um expediente armazenado no servidor. Como alternativa, os usuários podem colocar um cartão inteligente no leitor de cartões e utilizar uma impressão digital para autenticar que são titulares do cartão válido. O biométrico capturado pelo leitor se compara com os dados biométricos do cartão inteligente. Se a informação biométrica capturada iguala a informação biométrica armazenada no cartão, o cartão inteligente então libera a informação secreta requerida para registrar ao usuário na rede. Neste caso, a comparação biométrica pode fazer no leitor ou em um cartão (chamado match-on-card).

Figura 1 ilustra o processo biométrico de verificação de identidade.

Figura 1: Processo Biométrico de Verificação de Identidade



O valor de usar biometria para o acesso lógico incrementará à medida que a tecnologia se torna mais fácil e rápida para usar. As características pessoais são um atrativo, conveniente e confiável, do mecanismo de autenticação. As preocupações em matéria de segurança, entretanto, se centram no processo de combinação de informação biométrica, a qual regularmente se requer, já seja, que se envie informação não protegida a rede ou se armazene a informação no servidor anfitrião. Este tipo de informação é vulnerável para ser replicada (resultando em acessos ilegais) ou substituições (resultando em negação de acesso). Estas preocupações podem ser amenizadas ao proteger a informação biométrica em trânsito ou capturando e comparando os dados biométricos localmente (por exemplo, com um leitor ou um cartão inteligente).

Criptografia de chave pública

A criptografia dominante pública (também conhecida como criptografia dominante assimétrica) cifra a informação usando matematicamente pares relacionados de chaves criptográficas. Uma chave no par se utiliza para cifrar a informação; a informação, então, somente, poderia ser decifrada usando a outra chave. Os usuários obterão os pares dominantes de uma autoridade confiável e os utilizaram para intercambiar dados seguros e privadamente.

Cada par dominante abarca uma chave pública e uma chave privada. A chave pública se utiliza para cifrar a informação confidencial. A chave privada se deve manter secreta. A pessoa que usa a chave privada pode, portanto estar segura que a informação que a chave pode decifrar foi pensada para eles, e a pessoa que envia a informação pode estar segura que somente o que tem a chave privada pode descifrá-la.

A informação que descreve a chave pública se registra em um certificado assinado digitalmente por uma autoridade certificada. Um usuário pode proporcionar a chave pública a um remetente, ou a chave pode ser recuperada de um diretório no qual se publique.

O uso de chaves simétricas é apoiado por PKI. PKI é uma combinação de estándares, de protocolos e de software integrando pelo menos dois dos seguintes componentes:

- Uma autoridade certificada ou Certificate Authority (CA), que publica e verifica certificados digitais.
- Se gera e se publica uma autoridade do registro (RA), que verifica a identidade do solicitante antes de que um certificado digital seja gerado e assinado.
- Uns ou mais diretórios onde se armazenam os certificados (com suas chaves públicas) e as listas de revocação de certificados (CRL) são armazenados.

A chave pública criptográfica oferece um nível adicional de segurança, tomando em conta que não existem secretos compartilhados. Geralmente, o certificado de PKI se armazena em um computador de registro ou um dispositivo de armazenamento (por exemplo, um cartão inteligente) e se utiliza para cifrar a contra-senha antes de que se envie para ser autenticado.

Fichas Sensibles ou Soft Tokens¹

O meio utilizado para armazenar as chaves criptográficas é por si mesmo uma contra-senha cifrada, com sua contra-senha conhecida só pelo usuário. Cada vez que seja necessária uma ativação será preciso registrar a contra-senha para decifrar o conteúdo da "soft token". A copia não cifrada da chave de autenticação é apagada depois de cada autenticação.

As Soft Tokens (fichas sensibles) são arquivos de programas que contêm as chaves criptográficas usadas para a autenticação. Os usuários se autenticam na rede ao provar sua posse e controle desta chave criptográfica (usualmente armazenada em disco ou em algum outro dispositivo). Os dispositivos armazenam as chaves criptográficas eles mesmos, com uma contra-senha de conhecimento único do usuário. Cada vez que se ativa é requerido o registro de uma contra-senha que decifre o conteúdo da Soft Token. A copia não cifrada da chave de autenticação é apagada depois de cada autenticação.

As Soft Tokens são vistos como artículos de baixo custo, de fácil uso e descartáveis. Entretanto, este método de autenticação não é comumente portátil; os usuários devem estar localizados no computador de um cliente para que possam autenticar-se. Alguns Soft-Token oferecem mobilidade ao usuário, permitindo que as chaves sejam armazenadas nos servidores e descarregadas ao sistema do usuário segundo se necessite, ou empregando os componentes dominantes gerados das contra-senhas combinadas com os componentes dominantes armazenados nos servidores. As Soft Tokens apoiam-se em um cliente confiado e em um servidor de confiança. Além disso, o usuário deve ter outra chave para ter acesso ao Soft Token; senão, qualquer pessoa com acesso a máquina do cliente pode ser autenticada.

Tecnologia de Cartões Inteligentes

Quando é utilizada para o acesso lógico, a tecnologia de cartão inteligente vem geralmente de duas formas, um cartão de crédito ou um dispositivo USB, cada um com um processador incorporado. Em grande medida a

¹ *Electronic Authentication Guideline*, NIST Special Publication 800-63, Version 1.0, June 2004

forma mais popular é o cartão de crédito, devido a sua capacidade de incluir uma foto e informação corporativa visível e de receber outros mecanismos de segurança tais como uma contra-senha magnética ou código de barra.

Sem importar sua aparência, os cartões inteligentes se podem utilizar para implementar qualquer forma de autenticação descrita acima. Os cartões inteligentes têm a capacidade de:

- Armazenar de forma segura as contra-senhas
- Gerar pares de chaves assimétricos e armazenar de forma segura certificados PKI
- Armazenar de forma segura as chaves simétricas
- Armazenar de forma segura os arquivos raiz das fichas OTP
- Armazenar de forma segura as planilhas biométricas de imagem

Usar um cartão inteligente para armazenar contra-senhas é o uso mais simples que tem os cartões inteligentes para obter acesso lógico. As vantagens desse tipo de sistema são:

- Os usuários não têm que lembrar suas contra-senhas
- As contra-senhas armazenadas podem ser enormes e quase impenetráveis frente a algum ataque.
- O cartão pode se ativar por um número de identificação pessoal (PIN) ou biométrico si se requiere, agregando um valor de autenticação.
- Esta implementação é usualmente a que mais econômica resulta ao sistema.

Os cartões inteligentes podem, também, ser utilizados para apoiar esquemas mais poderosos de autenticação. Por exemplo, em um sistema que utilize chaves simétricas, o cartão pode armazenar uma informação secreta compartilhada implantada ao momento da fabricação.

Esta chave pode então utilizar durante o processo de autenticação um servidor seguro como parte da seção algorítmica de mudanças e de respostas. Os cartões inteligentes também se reconhecem amplamente como portadores ideais das credenciais de PKI; os cartões inteligentes podem armazenar certificados de chaves públicas com segurança, apoiar a geração de chaves no cartão (support on-card key generation) e proteger a chave privada do usuário.

O uso do cartão inteligente com um o mais desses enfoques pode proporcionar meios mais seguros de acesso lógico, ainda que a combinação, necessariamente, não preencha os critérios de dois ou três formas de autenticação.

Por exemplo, um cartão inteligente por si mesmo não pode autenticar a um usuário na rede, mas o cartão inteligente pode armazenar informação que proporcione um mecanismo de acesso. Um cartão inteligente que armazena o certificado da conexão PKI de um usuário pode autenticar ao usuário na rede preenchendo os requisitos que tenha o usuário. Entretanto, combinar um cartão inteligente com um PIN ou um cartão inteligente com ambos, um PIN e dados biométricos proporciona a autenticação de três formas.

O quadro 1 resume o uso do cartão inteligente com as formas de autenticação.

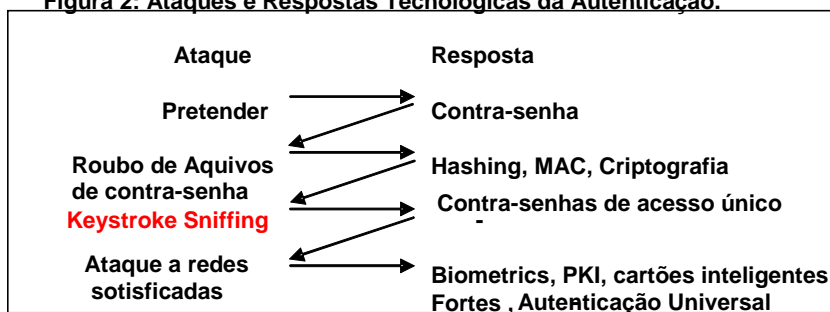
Tabela 1: Enfoques de Autenticação Individuais e Múltiplos

Acesso de Autenticação	Fatores		
	Algo que tenhas	Algo que saibas	Algo que sejas
Contra-senhas		✓	
Arquivo de fichas OTP ou "OTP" token seed file	✓		
Molde da imagem biométrica na base de dados			✓
Cartão Inteligente	✓		
Cartão Inteligente com PIN	✓	✓	
Cartão inteligente com certificado de registro PKI de cartão inteligente	✓		
Padrão de Imagem Biométrica armazenada no cartão inteligente	✓		✓
Cartão inteligente com PIN ou contra-senha (ou certificado) armazenada no cartão	✓	✓	
Cartão Inteligente com PIN, contra-senha (ou certificado) e biometria no cartão	✓	✓	✓

Resumo

Segundo se mostra no quadro 2, as tecnologias de autenticações têm sido uma forma complexa de resposta a novos ataques nos sistemas e redes. O propósito da tecnologia de autenticação é simplesmente o de não permitir o acesso não autorizado aos indivíduos a informação e aos programas, sem importar o seu propósito. Pois a informação chega a ser cada vez mais vital, é crítico que os indivíduos autorizados tenham os privilégios que permitam acesso a informação e aos programas que são apropriados e essenciais para suas funções e rol. Os ataques contra os sistemas têm sido criados segundo a necessidade de ter respostas tecnológicas que podem ser utilizadas para frustrar as instruções.

Figura 2: Ataques e Respostas Tecnológicas da Autenticação.



Fatores importantes a considerar para implementar uma autenticação mais poderosa de acesso lógico

Os negócios e as negociações estão descobrindo que o enfoque atual para a autenticação do acesso lógico é obsoleto e inadequado. Inúmeros fatores importantes estão levando as Companhias e as agências estatais a reavaliar as suas estratégias e planos lógicos de acesso, tendo como resultado uma tendência ao uso de uma autenticação mais poderosa baseada no acesso lógico. Esta seção revisa algumas das considerações e dos requisitos dominantes do negócio que conduz a esta tendência e discute como um método mais poderoso pode ajudar a encontrar estes requisitos.

Ambiente Corporativo

As mudanças no ambiente de negócios podem ser poderosos agentes para a re-engenharia dos processos tecnológicos e a implementação de uma autenticação mais poderosa no acesso lógico e físico.

- **Está sua empresa tentando adequar-se as novas regulações, tais como HIPAA, Sabanes-Oxley, Gramm-Leach-Bliley, Visa Waiver Program, ou a Associação Cívica Internacional de Aviação (em inglês ICAO), Machine-Readable Travel Documents (MRTD)?** Muitas dessas regulações afetam a aqueles que tomam as decisões, assim como ao Departamento de Sistemas de informação. Métodos mais poderosos de autenticação podem ajudar a tratar com os requisitos de acesso e auditoria que são integrais para estas regulações.

Por exemplo, fazer cumprir uma poderosa autenticação mediante o uso de cartões inteligentes e impressão digital biométrica podem ajudar a lidar com muitas das regulações privadas das HIPAA compliances.

- **Sua organização ou um sócio do negócio sofreu recentemente uma abertura na sua segurança ou tem realizado uma auditoria que não tem refletido a vulnerabilidade da sua segurança?** A pesar de que tais acontecimentos podem ser desagradáveis tem que lidar com eles. Estes podem prover uma motivação extra e financiamento que permita implementar poderosas medidas de segurança de acesso lógico onde seja necessário.
- **Está a sua organização completando, planejando, ou implementando um sistema de acesso físico novo ou melhorado? Você considera a integração a seus sistemas de acesso físico e lógico?** Considere atualizar seus procedimentos lógicos de acesso ao mesmo tempo. Ter uma vista integral dos requisitos de acesso pode oferecer-lhe um sistema de segurança poderoso, mais integrado e amigável. Os métodos de integração do acesso lógico e físico podem prover de igual forma economia significativa, eliminando ou reduzindo o número de placas ou cartões de identificação requeridos pelo sistema, evitando a troca dos leitores ou os custos de atualizar-los e aerodinamizar os procedimentos de provisão de identidade.
- **Esteve a sua organização implicada recentemente em uma aquisição ou uma fusão? Você se encontra integrado ou migrando múltiplos sistemas de informação?** Muitas companhias se enfrentam ao desafio de lidar com sistemas de acesso lógicos complicados ao integrar diferentes ambientes de Sistemas de informação. Muitos grupos rejeitam estas novas iniciativas até que se encontram integrados aos diferentes sistemas de informação. Mas este enfoque pode ser arriscado

e custoso no que se refere ao acesso lógico. Em seu lugar, considere a implementação de poderosas medidas de autenticação como uma ajuda na migração dentro do processo da integração. Por exemplo, uma poderosa autenticação posta em execução com uma só credencial de cartão inteligente poderia substituir o uso de múltiplos cartões de identificação e contra-senhas de usuários acrescentando segurança aos sistemas de informação.

Transformação do Negócio e Re-estruturação do Processo

Muitas organizações consideram uma poderosa autenticação como um componente contra contra-senha no prometo de re-engenharia de processos dos Sistemas de informação na companhia.

Formatted: Bullets and Numbering

- **Sua organização está considerando integrar a administração integral da identidade? Você está pensando em compartilhar suas credenciais de identidade com seus sócios, provedores ou as agencias estatais?** Se é assim tais planos podem ajudar a determinar que tipo de prática de autenticação se deve implementar com miras a conservação de seus sócios corporativos mostrando-os como estas práticas fortalecerão a administração da identidade de maneira global. Uma poderosa autenticação também será um componente integral de qualquer sistema de gerência federado no que você decida participar. Requerer o uso apropriado de uma poderosa autenticação em um sistema de gerência federado o protege não somente contra as debilidades potenciais dentro da sua própria organização, mas também contra debilidades potenciais em outras partes da federação.
- **Você tem uma estratégia web de serviços ou de emissão de serviços em curso? Responde esta estratégia a seus empregados, clientes ou a ambos?** A migração a uma infra-estrutura web cêntrica para ambas aplicações, internas e externas, representa uma oportunidade excelente de centralizar, integrar e consolidar políticas e práticas lógicas de acesso.
- **Sua organização está esperando substituir as identificações e contra contra-senhas de múltiplos usuários com uma só credencial?** Aspectos relacionados com o uso, gerência contra-senhas e as preocupações relacionadas com a segurança (Concernente ao re-uso ou uso de contra-senhas fáceis de lembrar) tem estimulado iniciativas de um registro único ou de um número reduzido de iniciativas de registro único em muitas organizações. Uma só credencial de registro único determina o uso de poderosos métodos de autenticação quando se utiliza esta “super” credencial.

Redução de Custos e Retorno da Inversão

A implementação de uma poderosa autenticação pode ajudar a reduzir os custos globais dos sistemas de informação e a obter um retorno obrigado da inversão. Entre as dúvidas sobre as contra-senhas a considerar temos:

- **Qual é o custo total de manejar identificações de usuários e suas contra contra-senhas ao largo de sua organização, incluindo custos intangíveis tais como satisfação do cliente e a produção do empregado?** Além dos riscos da segurança inerente no uso de identificações de usuários e suas contra-senhas, outros custos incluem a administração do sistema, a ajuda do posto de informação e a perda de produtividade. Os métodos poderosos de autenticação podem economizar o dinheiro ao mesmo tempo em que realizam segurança.

Entender o custo total dos atuais procedimentos lógicos de acesso podem ajudar a quantificar as vantagens de realizar uma migração a métodos de autenticação mais poderosos.

- **Quantas aplicações, sistemas e redes possuem, utiliza ou dirige sua organização? Quantos usuários acessam estas aplicações, sistemas ou redes?** Quanto mais sistema possua você e quanto maior seja a população de usuários, maior pode ser a economia alcançada ao migrar a um método de autenticação mais poderoso. Quanto maior economia de custo prover da segurança melhorada, a economia de custo administrativo pode contribuir de maneira significativa ao êxito do negócio.
- **Como está formada sua população de usuários? Podem seus sócios de negócios acessarem seus sistemas? Os usuários têm acesso a seus sistemas desde redes externas?** Quanto mais variada seja sua população de usuários, maior é o retorno na inversão como resultado da migração a métodos mais poderosos de autenticação. Tal migração oferece a flexibilidade de eleger e de fazer cumprir os procedimentos mais eficazes de autenticação para cada variedade de usuário. Por exemplo, a autenticação de duas formas (tal como um cartão inteligente e uma biometria) se pode requerer para alcançar o acesso remoto a uma internet, ao mesmo tempo que, somente, mediante uma só forma de acesso (tal como um cartão inteligente e uma biometria) se pode requerer para o acesso de rede localizado no campo universitário.

Segurança e Privacidade

Melhorar a segurança do acesso aos Sistemas de informação e proteger a privacidade dos indivíduos são as principais prioridades das organizações que implementam novos sistemas de acesso lógico que utilizam poderosas técnicas de autenticação. Entre os fatores que encorrem no uso de contra-senhas a considerar temos as seguintes interrogantes:

- **Sua organização tem política de privacidade que proteja a informação do usuário contra o acesso desautorizado?** Por exemplo, os administradores de sistema não devem poder filiar a informação pessoal dos usuários segundo seja sua vontade. Os poderosos procedimentos de autenticação podem permitir aos administradores realizar plenamente suas tarefas ao mesmo tempo em que prevê que esses acessam informação confidencial dos usuários.
- **Seus métodos existentes de autenticação proporcionam suficiente segurança e privacidade? Sua segurança de acesso lógico depende somente de contra-senhas?** O controle de acesso pode ser fortalecido usando múltiplas formas de autenticação (algo que você tem, algo que você sabe e algo que você é). Níveis mais altos de segurança e privacidade alcançam quando os métodos de autenticação utilizam formas de varias categorias (por exemplo, biometria múltipla). Um sistema poderoso de autenticação corretamente implementado pode fazer cumprir uma variedade de políticas e procedimentos da autenticação, baseado nas necessidades particulares das aplicações utilizadas e nas necessidades da população de usuários.
- **Sua organização utiliza placas ou cartões de identificação? Como se produzem e se distribuem esses cartões?** Os poderosos procedimentos de autenticação podem nivelar e melhorar uma infraestrutura existente de um cartão de identificação emitida e se pode

implementar usando a produção central ou distribuída do cartão. A produção e a distribuição central proporcionam uma segurança agregada e reduz os custos de equipagem e de manutenção. Distribuir a produção desde o ponto de inscrição proporciona um rápido retorno, aumenta a satisfação do cliente e representa uma oportunidade adicional de capacitar aos usuários.

- **Está pronta a tecnologia biométrica para ser utilizada? Que aplicação biométrica é a correta para seu sistema?** Os provedores da tecnologia biométrica continuam logrando avanços em exatidão, funcionamento e custo. Os sistemas biométricos de hoje oferecem capacidades compatíveis, usáveis e aceitáveis, ao mesmo tempo em que proporcionam um funcionamento fiável e confiável para os usuários do sistema. É importante selecionar a tecnologia biométrica que é apropriada para o requisito de uso e de autenticação. Se a impressão digital, o diafragma, a voz, a cara, algum outro fator biométrico ou a biometria múltipla são usadas, a tecnologia biométrica pode ajudar a fazer cumprir níveis mais altos de segurança e de privacidade no sistema lógico de acesso, ao mesmo tempo em que também proporciona benefícios úteis.

Gerência, Uso e Capacitação

As soluções poderosas de autenticação podem simplificar a administração e melhorar a utilidade dos processos de autenticação. Considere as perguntas seguintes ao implementar novas soluções de controle de acesso.

- **Como sua organização detecta e desativa as credenciais perdidas ou roubadas? Como você sabe quando está comprometida uma contra-senha?** Estes problemas sérios para as aplicações de acesso lógico, especialmente se estes se encontram protegidos por contra-senhas fixas. Uma autenticação poderosa reduz ao mínimo esses riscos. Por exemplo, requer o uso de um cartão inteligente e de uma contra-senha que reduz ao mínimo os riscos que uma contra-senha será compartilhada ou comprometida. Usar dados biométricos com um cartão inteligente de forma eficiente faz o cartão inútil se se perde ou se rouba.
- **Como sua organização capacita a seus usuários em segurança?** A capacitação em segurança é um elemento importante da segurança total de qualquer organização. Uma autenticação poderosa proporciona um constante lembrete aos usuários, de que a segurança é importante. Também oferece uma oportunidade adicional de capacitar os usuários na temática de segurança. Por exemplo, durante a emissão dos cartões de identificação, os usuários podem ser capacitados no uso apropriado de suas poderosas credenciais de autenticação. Esta capacitação pode incluir uma demonstração de como apresentar uma impressão digital de alta qualidade e descrever como se protegem e se armazenam os dados biométricos, e quem tem acesso a eles. As credenciais fortes de autenticação são também um lembrete para os empregados de que as atividades da rede estão sendo supervisionadas e que a segurança da rede e dos computadores é extremamente importante.
- **Sua organização tem áreas de trabalho comum ou de acesso de turnos rotativos que requerem que as estações de trabalho sejam utilizadas por vários usuários?** Um problema comum da segurança nestes tipos de ambientes é a carência dos controles de acesso do usuário ou o compartilhar as credenciais do usuário. Os usuários

encontram comumente maneiras de evitar os controles de acesso incômodos que atrasem o fluxo do trabalho. Uma poderosa autenticação pode ajudar a proporcionar uma melhor segurança para os administradores dos sistemas de informação e uma melhora na utilidade para os usuários, resolvendo as necessidades de ambos grupos. Por exemplo, usar uma impressão digital para assinar uma transação prove aos administradores de um controle e de um rastro de intervenção de um usuário individual, ao mesmo tempo em que também se converte em uma maneira de acesso mais rápida e mais fácil para o usuário que logea e desloga utilizando um nome de usuário e uma contra-senha.

- **Quantas identidades necessitam administrar os usuários hoje em dia? Quantas identificações de usuários e contra-senhas devem esses lembrar?** Em quase todos os trabalhos e indústrias, os usuários devem interagir com inúmeras aplicações. A mesma está conformada pela frequente tendência ao fornecimento eletrônico das vantagens, comunicações e treinamento dos empregados. Assim que não somente necessita usuários para administrar identidades para o fluxo de trabalho e os processos das aplicações, mas devem também lembrar a princípio, as identidades dos usuários e contra-senhas para os recursos humanos, o cuidado médico e os usos financeiros também. Uma poderosa autenticação pode ajudar a simplificar a administração de identidades para os usuários e os administradores ao mesmo tempo em que proporciona níveis mais altos de segurança.

Benefícios que Oferece a Tecnologia de Cartões Inteligentes para o Acesso Lógico.

Para a maioria das organizações atuais, o computador e os recursos de rede são acessados utilizando uma identidade de usuário e uma contra-senha. Cada sistema ou aplicação assigna comumente uma identidade de usuário e uma contra-senha para esse usuário baseando-se nessa identidade única do usuário. As identidades dos usuários são administradas por uma aplicação. Entretanto, como o número de sistemas e usos em uma organização cresce, o administrar que utiliza essas identidades cria significativas ineficiências operacionais. O aumento do número de aplicações introduz debilidades na segurança ao mesmo tempo em que se faz mais difícil o implementar regulações no uso daquelas identidades.

Autenticação Forte

Mais e mais organizações buscam soluções para autenticações mais fortes que vão mais além do uso de nomes de usuários e contra-senhas de acesso para validar que os sistemas de acesso dos usuários são de quem eles dizem ser. As organizações que desenvolveram poderosas autenticações (comumente em forma de símbolos dinâmicos) tradicionalmente oferecem essa solução só aos empregados que a acessam remotamente. Esta prática está baseada em assumir que os indivíduos que estão dentro de um edifício são confiáveis. Entretanto, o 2004 E-Crime Watch Survey (desenvolvido pela Revista CSO em cooperação com o serviço Secreto de Estados Unidos e o CERT Coordination Center) revelou que 36% dos 350 pesquisados experimentaram “acesso não autorizado por alguém de dentro” como um dos crimes eletrônicos cometidos contra sua organização em 2003. Este tipo de crime foi o quarto ataque mais comum, atrás de vírus, negação de serviços e spam. IDC estima que mais de 60% de todas ameaças internas

provém dos empregados, contratistas, consultores, integradores de sistemas, sócios, distribuidores e outros com acesso privilegiado .

As fronteiras dos sistemas de informação e data continuam expandindo-se. A tecnologia de internet e as tecnologias inalámbricas proven um crescente número de pontos de acesso convenientes a empregados, mas criam um pesadelo para o departamento de sistemas de informação.

Para indicar a segurança em uma organização, se necessita um método para prover uma poderosa e consistente autenticação para o acesso a todos os recursos de rede. A tecnologia de cartões inteligentes é a maior plataforma para assegurar todos os pontos de acesso em uma organização.

Os cartões inteligentes aumentam significativamente a segurança das credenciais digitais de um usuário à margem da natureza das credenciais. As credenciais são armazenadas permanentemente em um cartão, o qual está em posse do usuário final e nunca disponível em software ou na rede para que um usuário não autorizado a roube. Os cartões inteligentes são em geral usados para permitir dois fatores de autenticação, incorporando algo que você tem (o cartão inteligente) e algo que você não conhece (comumente um PIN que ativa as funções criptográficas do cartão). Tomar o controle da identidade digital de um usuário requer roubar o cartão inteligente e adivinhar o PIN. Os usuários se percatam rapidamente de quando um cartão é roubado e podem contatar ao administrador de rede para revocar as credenciais roubadas. Adicionalmente, muitos intentos falidos de adivinhar a contra-senha do cartão podem fazer que este se bloqueie.

A tecnologia dos cartões inteligentes também apoia as tecnologias biométricas (algo que você é) habilitando a autenticação com três elementos. Como uma alternativa, a biometria pode simplesmente substituir o PIN, o qual ao mesmo tempo em que reforça a segurança incrementa a conveniência do usuário. Acrescentando a autenticação biométrica a controle de acesso é fácil, posto que o cartão inteligente pode armazenar a informação biométrica do usuário e levar a cabo o processo requerido para determinar uma combinação. Nenhuma base de dados back-end de dados biométricos é requerida. Contar com as credenciais para acessar uma aplicação armazenada de forma segura e protegida pela informação biométrica do usuário, prove a uma organização com segurança biométrica, sem ter que experimentar aplicações back-end.

Segurança Incorporada ao Sistema

Um cartão inteligente é tipicamente um dispositivo do tamanho de um cartão de crédito com um processador de computador incorporado. O processador pode conter um micro-controlador com uma memória interna ou somente a memória. Os processadores inteligentes também podem estar incorporados em outros dispositivos, incluindo as fichas que se conectam diretamente ao porto USB e a processadores SIM que se conectam a celulares GSM.

Os processadores micro-controladores são a eleição mais prática para as aplicações de acesso lógico seguro, devido a que esses processadores podem armazenar grandes quantidades de informação e têm a habilidade para processar informação e realizar uma variedade de funções. Esta habilidade única apoia a adição de métodos ativos de segurança aos cartões inteligentes, dependendo dos requerimentos da aplicação. A maior parte das soluções do cartão inteligente atualmente disponível para o acesso lógico está já carregada com os algoritmos encriptados mais utilizados, tais como DES, 3DES e RSA .

Além disso, a maioria dos micros controladores baseados em cartões inteligentes são decontra-senhados para resistir ataques. Os fabricantes inteligentes constroem uma variedade de contramedidas que detectam e reacionam a um número de possíveis ataques, incluindo voltagem, frequência, manipulações da luz ou temperatura e impulso elétrico diferencial ou estadístico. A reação típica da maioria dos ataques é a de bloquear o cartão, fazendo-o inoperável.

Os ataques sofisticados aos cartões inteligentes são caros e consomem tempo e o atacante deve ter em mãos o cartão. Se o cartão inteligente de um usuário se extravia, este deve ser reportado, e em seguida é inabilitado antes que qualquer ataque possa ter lugar. Quando as credenciais são armazenadas em um programa ou no computador de um usuário, entretanto, o usuário nunca poderia saber que está sendo roubado.

Aumento da Segurança e Conveniência para Usuários

Os usuários na maioria das organizações enfrentam o reto de manejar múltiplas contra-senhas de ingresso para múltiplos sistemas e aplicações. Este requerimento tem aplicações para a segurança e a produtividade do usuário. Alguns departamentos de sistemas de informações elegem o caminho de menor resistência, permitindo aos usuários usar a mesma contra-senha para cada aplicação. Esta prática representa o maior risco de segurança, posto que todas as aplicações são comprometidas se uma só contra-senha é adivinhada ou roubada. Outros departamentos de sistemas de informação poderiam estabelecer uma política mais forte, requerendo uma contra-senha diferente para cada aplicação e uma contra-senha mais complexa que tenha uma mistura de tipos de caracteres (alfanumérica, maiúscula, minúscula, símbolos). Adicionalmente, uma política segura de contra-senha poderá requerer que as contra-senhas fossem trocadas cada certo tempo. Estabelecer políticas mais fortes relacionadas às contra-senhas de ingresso é um passo importante quando o acesso depende de uma só contra-senha fixa, mas reforçar estas políticas pode ser um reto. A maioria dos usuários tem dificuldade para lembrar contra-senhas de ingresso complexas, por isso eles escrevem ou armazenam em um texto de seus computadores, onde podem ser facilmente roubadas.

Os departamentos de informação também se enfrentam de igual maneira com o desafio de administrar as contra-senhas para múltiplos usuários e múltiplas aplicações sem ter que sacrificar a produtividade e sem criar usuários insatisfeitos. As estatísticas da indústria mostram que dos 30% aos 50% dos recursos auxiliares de IT são consumidos na administração e resignação de contra-senhas. A produtividade final do usuário também é afetada, posto que não pode ter acesso as aplicações até que não se assigne uma nova contra-senha.

Varias “administrações de identidade” estão disponíveis para manejar esses assuntos de produtividade. Consolidar as identidades dos usuários em diretórios centrais e implementar ferramentas provisionais para administrar essas identidades minimizam as perdas de produtividade ao fato de ter que manejar diferentes identidades para diferentes contas. Este tipo de solução também enfoca as vulnerabilidades de segurança possuídas pelas contas que permanecem em um sistema logo de que o acesso do proprietário já não é válido. Soluções similares estão disponíveis para os conteúdos WEB e aplicações. Entretanto, este tipo de solução não pode ser implementada da noite para o dia. Adicionalmente, elas requerem uma mudança gradual na infra-estrutura de organização back-end. E os usuários seguiriam

necessitando **to juggle** múltiplas contra-senhas de ingresso para suas aplicações. Outras soluções para o manejo de identidade simplificam a experiência final do usuário ao usar a sincronização de contra-senhas de ingresso, auto serviço de administração de contra-senha, or Acesso único, mas estas também requerem regulamente modificações a infra-estrutura do sistema de informação e não enfocam as preocupações de segurança derivadas do uso de contra-senhas de ingresso.

As organizações que usam a tecnologia de cartão inteligente para acesso lógico não tem que esperar pela implementação de sistemas de gerência back-end para dar-se conta das eficiências operacionais e o retorno da sua inversão. As identidades e as credenciais do usuário podem ser consolidadas em um cartão inteligente imediatamente, provendo ao usuário uma simples e consistente aproximação ao acesso lógico, independentemente de que o usuário esteja conectado a uma estação de trabalho ou a uma rede ou acessando a uma rede remotamente utilizando um VPN. O resto da experiência do usuário se mantém constante quando a organização coloca ao dia sua infra-estrutura de administração de identidades: insira um cartão inteligente e insira seu PIN.

Um cartão inteligente é a chave pessoal do usuário para toda a sua informação e aplicações. Adicionalmente, devido a que a chave é portátil, os usuários não estão atados a uma só estação de trabalho na qual as credenciais estão localizadas. Podem ir de máquina em máquina, uma vantagem crítica para usuários que trabalham em múltiplos lugares.

Proteção Aumentada contra Fraudes de Identidade

Os cartões inteligentes podem ajudar a defender-se, cada vez mais, contra os ingeniosos atentados de **“phishing”**. O **“phishing”** usa uma mensagem de Internet para tentar enganar aos indivíduos para que divulguem a informação de suas contas. Por exemplo, uma tentativa de **“phishing”** poderia usar e-mail enviado a uma vítima potencial, que parece ser uma ingênua petição de alguém confiável (por exemplo, um banco ou um provedor de serviços de internet) o indivíduo poderia então responder a petição oferecendo números de contas, PINs ou contra-senhas de ingresso a um sitio web enganoso que se faz passar como uma identidade legítima. Os ataques de **“phishing”** se aproveitam da falta de autenticação entre o que envia o e-mail e o destinatário y entre sitio web enganoso e o indivíduo.

Os cartões inteligentes podem ser usados para combater os ataques de **“phishing”** ao aplicar mutua autenticação de dupla vía para assegurar o acesso aos serviços do sitio web. Quando os emissores de contas oferecem um serviço de web (por exemplo, para administração de contas), eles podem emitir cartões inteligentes de forma que permita aceder ao sitio web verdadeiro. A credencial do cartão inteligente pode autenticar ao usuário para o sitio web e autenticar o sitio web como legítimo.

Ao prover uma autenticação firme e universal, ao permitir a autenticação mútua, os cartões inteligentes podem ajudar a combater os ataques de **“phishing”**. Pode-se assegurar aos indivíduos que eles estão se comunicando com um sitio legítimo e que suas credenciais de identidade estão sendo protegidas contra o acesso não autorizado.

Cobertura de Aplicações baseadas em Estándares

A tecnologia dos cartões inteligentes está se convertendo no método preferido para o acesso lógico, não somente pelo incremento da segurança

dos cartões inteligentes, mas também pelo seu fácil uso, amplia cobertura de aplicação, facilidade de integração e funcionalidade universal.

Os cartões inteligentes oferecem às organizações uma solução custo-efetiva que pode ser desenvolvida facilmente e a qual é aceita, de forma ampla, pelo usuário final.

Diferentes aplicações impõem diferentes requerimentos dos usuários antes de permitir a eles o acesso. Algumas aplicações apoiam só um método para garantir o acesso; outras apoiam vários métodos. Poucas aplicações permitem que as credenciais sejam compartilhadas.

Alguns dos mais comuns métodos de acesso as aplicações sai uma combinação do nome do usuário e a contra-senha, só a contra-senha, um segredo compartilhado, OTP, biométricos e PKI ou certificado digital. A combinação do nome do usuário e a contra-senha, com tudo e que é a aproximação menos segura, é atualmente o método primário usado para o controle de acesso. Métodos mais seguros, tais como OTPs ou certificados PKI, podem incrementar a segurança só para aplicações que apoiem esses métodos e requeram infra- estrutura adicional para administrar-se.

Na medida em que os métodos multiplicam os requerimentos para aceder as aplicações, a aceitação dos usuários decresce, o qual ao início leva a um decréscimo na segurança.

Os cartões inteligentes, a diferença de outras soluções, podem prover ao usuário com todos estes métodos de acesso em um só cartão, e para acessar só requer o PIN do usuário.

A unicionalidade adicional permite que os cartões inteligentes gerem OTPs que substituem o PIN. Os produtos comerciais estão disponíveis a oferecer a segurança aos cartões Inteligentes para armazenar nomes de usuários e palavras de ingresso para todas as aplicações. Somado a essa, os cartões inteligentes são mais flexíveis que a tradicional tecnologia de fichas, devido a que são dispositivos criptográficos que podem apoiar uma ampla gama de funcionalidades. Ela não depende da presença de um servidor e elas podem ser apagadas e reprogramadas para seu uso continuado dentro de uma organização.

Os cartões inteligentes podem agora prover a um usuário com uma só interface aceder a todas as aplicações independentemente das credenciais requeridas para a aplicação. Isto incrementa a aceitação e conveniência para o usuário e ao mesmo tempo implementa e reforça as políticas de segurança da organização.

Nos últimos anos, os padrões têm evoluído ao ponto de que provêm a inter-relação da operação necessária para permitir ao cartão inteligente aceder a vários recursos da organização. Por exemplo, padrões criptográficos, tais como PKCS#11 e Microsoft Crypto API (CAPI) permitem aplicações para usar um certificado digital armazenado em um cartão inteligente para autorizar o acesso ao usuário final.

A contra-senha privada é armazenada no processador do cartão inteligente e só pode ser acessada por um usuário que tenha o PIN correto quando a aplicação abre.

A união do computador pessoal/cartão inteligente (PC/SC) e a proliferação de leitores, e drivers de leitores, têm contribuído também para que exista uma aceitação mais ampla dos cartões inteligentes para o acesso lógico.

O preço dos leitores tem diminuído, e sua capacidade e disponibilidade vêm incrementando, ao ponto de que muitos dos principais fabricantes de computadores agora incorporam um leitor ao teclado de um computador ou de uma portátil por um pequeno custo adicional.

Fácil de Integrar

Os cartões inteligentes incluem funções incorporadas que simplificam a sua integração na infra-estrutura do sistema de informação de uma organização. A maioria das aplicações que requerem outras credenciais, a parte do nome do usuário, encaixam em um dos padrões citados acima. Por esta razão, permitir o acesso do cartão inteligente é, geralmente, simples, requerendo, somente, a instalação de uma aplicação administrativa de nível médio no computador. Os cartões inteligentes podem então ser usados para registrar-se ao sistema, ter acesso VPN, ingressar e encriptar correio eletrônico, acesso a web baseado em SSL, e para o registro baseado em dados biométricos.

A maioria dos líderes CAs tem adotado os cartões inteligentes como a plataforma preferida para armazenamento e uso de certificados digitais. A CA pode usar já seja os PKCS #11 ou a interface Microsoft CAPI para gerar chaves, carregar certificados e realizar as requeridas funções criptográficas. Configurar uma CA para usar um cartão inteligente consiste, comumente, em selecionar a correta interface.

Os leitores dos cartões inteligentes agora estão facilmente integrados com o uso do sistema operativo de escritório com dois padrões: o PC/SC padrão e o CCID(Chip Card Interface Device).

O padrão do PC/SC permite que se integrem os leitores de cartões inteligentes, facilmente, com programas de nível médio ou com outras aplicações, sem importar o fabricante ou o sistema de comando. Apesar de que este padrão foi desenvolvido para ser usado no ambiente da Microsoft, agora é considerado, de fato, o melhor padrão para muitas outras plataformas.

A especificação do CCID foi desenvolvida para os leitores de cartões inteligentes USB. Foi desenvolvida para apoiar a integração fácil dos leitores de cartão inteligente com os sistemas operativos de escritório, de tal modo que evita a necessidade de instalar um software adicional ao driver do leitor do usuário. A especificação foi definida pelo USB Implementer's Forum (USB-IF) juntamente com a indústria de cartões inteligentes. A CCID define um sistema de comando e um protocolo de transporte sobre o USB de modo que um sistema hóspede possa se comunicar com um leitor de cartões inteligentes. Uma classe específica de USB está definida, agora, para leitores de cartões inteligentes.

A adoção da especificação do CCID permite aos fabricantes dos leitores de cartões inteligentes construir os dispositivos que são compatíveis com esta especificação. Os vendedores do Sistema operativo podem escrever um driver que se agrega a esta especificação e apoiar a todos os leitores CCID compatíveis. Microsoft lançou um driver CCID compatível com a atualização do Windows, para o Windows 2000 e Windows XP. O driver será incluído em pacotes de serviço e em todos os lançamentos futuros do sistema operativo. Enfoque no Windows CE está, também, sendo considerado. Outros vendedores importantes dos sistemas operativos (exemplo, Apple e Sol) também estão incluindo drivers nativos do CCID em seus sistemas operativos.

O uso de um leitor de cartões inteligente CCID compatível proporciona um verdadeiro apoio ao plug-and-play, removendo qualquer necessidade de que um programa adicional seja instalado. Isto põe em vista a experiência do usuário.

A Figura 3 mostra uma variedade de soluções para conectar um cartão inteligente a um computador, incluindo leitores de cartões inteligentes sem contato e com contato, dispositivos USB e um leitor de cartões inteligentes com o leitor biométrico integrado.

Figura 3: Exemplos de leitores de cartões inteligentes²



Fácil de Distribuir

As ferramentas de administração e os métodos de distribuição estão disponíveis permitindo a grande emissão de cartões inteligentes. Os sistemas administrativos integrados no diretório de um sistema de compras proporcionam a função requerida para emitir e administrar os cartões inteligentes e suas credenciais. Os drivers do leitor e os programas de nível médio do cartão inteligente são maduros e facilmente distribuídos através de uma organização.

Ambos apoios: o de administração de alto nível e a administração dedicada de projetos são aspectos críticos para uma implementação com êxito. Distribuir um novo sistema de administração de identidades que incluam cartões inteligentes pode ser um projeto complexo que se estende através de várias organizações e afeta as habilidades básicas do negócio.

Função Universal

Os cartões plásticos são acessórios comuns dentro de muitas organizações e têm muitas aplicações, tais como: identificação, acesso físico,

² Photos provided by Atmel, Axalto, Datakey, Gemplus, Honeywell, and SCM Microsystems. Additional information about smart card readers can be found in the Smart Card Alliance smart card reader catalog at www.smartcardalliance.org.

administração do tempo e da assistência. Os cartões inteligentes permitem que as organizações combinem todos esses usos em um só cartão. O usuário pode então levar um só cartão para o acesso físico, o acesso lógico, a identificação e outras funções do negócio.

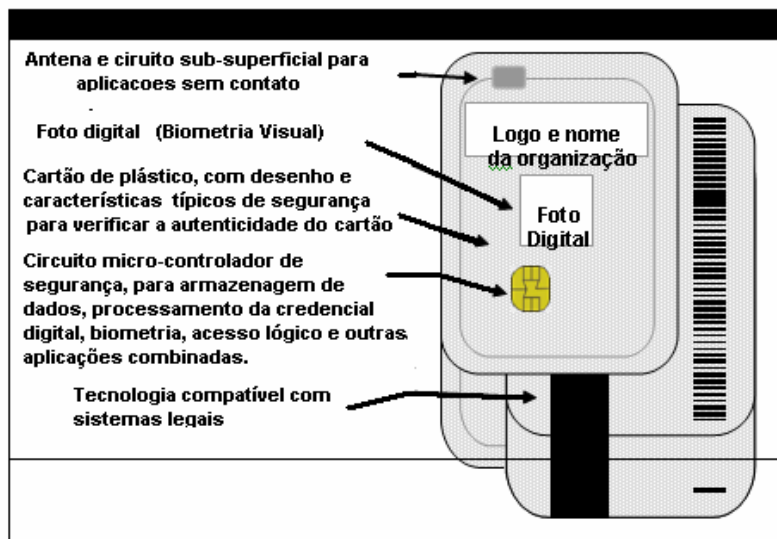
Outras tecnologias associadas geralmente a um cartão plástico tais como os magnéticos, códigos de barra, tecnologia da radio frequência (RF), e laminas de segurança podem ser utilizadas conjuntamente com o cartão inteligente. Além disso, assim como a tecnologia de circuito inteligente continua avançando nas capacidades sem conexão, os cartões inteligentes podem abarcar aplicações que requerem o uso de identificações sem contato, tal como o acesso físico aos edifícios e aos serviços de transportes.

Os cartões inteligentes que permitem a identificação sem contato se descrevem, geralmente, como micro-circuitos ou processadores híbridos ou de interfase dual dos cartões inteligentes. Um cartão híbrido contém dois processadores, um que se apóia em uma interfaz de contato e um que se apóia em uma interfaz sem contato. Os processadores geralmente não estão conectados. Um cartão com um micro-circuito de interfaz dual contém um processador simples permite ambas funções, uma interfaz de contato e uma sem contato com um só processador em um só cartão, com desenhos correntes que permitem que a mesma informação seja acessada usando, já seja, leitores com contato ou leitores sem contatos.

A maioria das organizações que utilizam, atualmente, os cartões inteligentes para o acesso físico e lógico tem emitido cartões inteligentes híbridos, usando a interfaz sem contato para o acesso físico e a interfaz de contato para o leitor de cartões inteligentes estándar da PC/SC no computador do usuário para o acesso lógico. Isto é porque, até pouco tempo, a tecnologia inteligente sem contato dos cartões não podia suportar aplicações que requeriam um alto nível de segurança e aplicações baseadas em encriptação, além do que a infra-estrutura requerida para apoiar a implementação do sistema sem contato para o acesso lógico (os usos e os leitores) não estava disponível. Hoje, os fabricantes de processadores inteligentes estão começando a fabricar processadores de interfaz dual com as capacidades de processamentos e rendimento requeridas para apoiar os mais sofisticados usos do acesso lógico. Os cartões de interfaz dual estão agora disponíveis como FIPS140-2, de nível 3 (como um cartão terminado) ou de cc. EAL 5+ (como um circuito integrado). Estes níveis de segurança são tão elevados que somente estão disponíveis nos cartões inteligentes. Os vendedores de aplicações estão desenvolvendo aplicações de acesso lógico que utilizam esses processadores em formatos de contato e sem contato. Ademais, os principais vendedores de leitores de cartões inteligentes estão começando a oferecer leitores estandarizados de cartões nos computadores, que se comunicam em qualquer modo.

A Figure 4 ilustra os componentes de um típico cartão de identidade inteligente.

Figura 4: Exemplo de Cartões de Identificação Inteligentes



Cartões Inteligentes Usados como Crachás de Identificação Inteligente: Exemplo de Cenário

Para ilustrar o que acontece quando as organizações proporcionam aos empregados um cartão inteligente de identificação que se utiliza para o acesso lógico e físico, considere um dia típico na vida de Kay Smith, o encarregada fictícia do serviço ao cliente de uma companhia fictícia, Enterprise Systems. O Enterprise Systems implementou um sistema de identificação inteligente para seus empregados há 2 anos, para integrar a segurança a organização e para cumprir com a política corporativa existente de segurança.

Antes da Enterprise Systems adotar o sistema de crachá de de identificação inteligente, o estacionamento da companhia era acessado usando um cartão magnético. As novas identificações inteligentes incluem fitas magnéticas de forma tal que a Enterprise Systems pode continuar utilizando seu sistema de acesso ao estacionamento. Ao iniciar o seu dia, Kay Smith tem acesso ao estacionamento que ela usa da mesma maneira de sempre, passando seu cartão através de um leitor.

Uma vez dentro do edifício, Kay deve apresentar o seu cartão inteligente de identificação ao segurança para verificar que o cartão é de fato seu. O segurança verifica a foto do cartão e indica que prossiga. Depois, Kay passa seu cartão perto do leitor de RF (radio frequência) que está na porta da recepção, assim que ela pode deixar o corredor e entrar na área principal do mesmo. Os sistemas da empresa podem manter seus leitores existentes de acesso por RF e incorporar a capacidade de acesso físico ao cartão inteligente de identificação. Os novos cartões inteligentes de identificação vêm com antenas RF integradas, que são inter-operáveis com os leitores. A única transformação para os empregados é que agora utilizam o mesmo cartão para acessar ao estacionamento da companhia e a área principal desta.

Agora que Kay está no seu escritório, ela liga seu computador e coloca seu cartão no leitor de cartões inteligentes incorporado ao aparelho. O processo padrão da conexão do Windows reconhece o leitor de cartões inteligente e pede a Kay inserir o PIN para o seu cartão, que somente Kay sabe. Kay, agora, entra na rede pelo seu computador e pode trabalhar. Como ela tem acesso a várias aplicações (exemplo: e-mail, base de dados do cliente, base de dados de suporte técnico) o computador pede uma contra-senha ou outro tipo de identificação. O cartão de identificação inteligente proporciona automaticamente a informação requerida para ter acesso a essas aplicações, e o único que Kay tem que fazer é entrar com o PIN inicial de identificação do cartão. Antes que a Kay lhe fosse dado o novo cartão, ela tinha que lembrar 12 distitas contra-senhas para diversos usos corporativos que a frustravam. Antes ela escrevia as suas contra-senhas em um caderno ao lado do seu computador. Kay ama seu novo cartão porque o processo agora é igual para ela, não importa a qual uso ela tem acesso. O cartão inteligente de identificação é também configurável de modo que o sistema da empresa pode requerer diversos processos ou as credenciais de autenticação para cada uso, se for necessário (por exemplo: requerendo o PIN de entrada do cartão inteligente para cada uso).

Kay está aderida a certas políticas de correio eletrônico da sua companhia. As mensagens de correio eletrônico com informação delicada relacionadas com informação de novos produtos ou assuntos relacionados a recursos humanos, devem ser registradas e encriptados. O sistema automaticamente acessa a informação relacionada a assinatura digital do cartão de identificação de Kay. Os sistemas da empresa usam certificação digital para o correio eletrônico. Para estar segura, Kay acessa as opções de segurança para a mensagem e tecla em "assinar e encriptar." O sistema tem acesso automaticamente a informação digital da assinatura sobre o cartão inteligente de identificação de Kay. Somente o usuário validado pode abrir e ler a mensagem de Kay.

É também uma política da empresa que os empregados devem levar seus cartões inteligentes de identificação sempre com eles. Kay vai até uma reunião e leva consigo o seu cartão. Uma vez o cartão se retira do leitor do escritório, o quadro do escritório de Windows não pode ser acessado até que Kay volte, reinserte seu cartão e entre com seu PIN de novo.

Em casa ao final do dia, Kay decide ter acesso a seu e-mail e também decide confirmar um pedido do seu cliente. Os sistemas da empresa utilizam os certificados digitais para o acesso de VPN. Kay utiliza seu cartão inteligente conjuntamente com um cliente de VPN no seu ordenador pessoal para conectar-se com a rede interna da empresa. A única informação que ela necessita proporcionar é seu PIN, e estará conectada.

Durante o curso do seu dia laboral, Kay utilizou um só cartão inteligente de identificação substituindo os vários cartões que necessitava para o acesso físico das instalações. O mesmo cartão tem facilitado e assegurado o acesso aos recursos de informação, permitindo utilizar esses recursos mais eficientemente. Como se ilustrou, os cartões inteligentes são um avanço eficiente para combinar segurança com facilidade de uso.

As Vantagens Sobre Outras Alternativas de Acesso Lógico

A tabela 2 resume as vantagens que os cartões inteligentes podem prover para o acesso lógico quando são utilizados com diferentes mecanismos de autenticações.

A tecnologia de cartões inteligentes representa um meio flexível e rentável para implementar qualquer técnica de autenticação. A tecnologia oferece vantagens tanto para o usuário do cartão como para o que emite, melhorando a experiência de ambos, ao mesmo tempo em que fortalece a autenticação e segurança do acesso lógico.

Tabela 2: Realçando a Autenticação com Cartões Inteligentes

Mecanismo de Autenticação	Característica	Valor agregado pelos cartões Inteligentes
Fator Único de Autenticação		
Contra-senhas Fixas de Acesso	<ul style="list-style-type: none"> • Fácil de adivinhar, rastrear ou roubar • Dificuldade para reforçar as políticas com contra-senhas seguras de ingresso • Frustração do usuário e dificuldade ao mudar e memorizar palavras de ingresso • De difícil administração 	Um sistema de cartões inteligentes provê um depósito seguro para contra-senhas de ingresso e automatiza o acesso do usuário, liberando ao mesmo dos requisitos para administrar contra-senhas. As políticas das contra-senhas de acesso são fáceis de implementar.
Ficha passivo ou ativa sem um PIN	<ul style="list-style-type: none"> • Ficha perdida ou roubada 	Um sistema de cartão inteligente prove a segurança para a ficha básica (Token seed) e adiciona também o acesso PIN ao cartão, executando o fator de autenticação forte
Leitor biométrico	<ul style="list-style-type: none"> • Resposta ao Ataque • Ataque encuberto • Credencial Biométrica e segurança combinada 	O sistema de cartão inteligente prove o armazenamento seguro do padrão biométrico, executa o dado biométrico no cartão, e adiciona o acesso PIN ao cartão, executando a autenticação de três fatores.
Dois fatores de Autenticação		
Contra-senha de acesso único e ficha com PIN	<ul style="list-style-type: none"> • Complexa infra-estrutura • Figura no meio de um ataque • Produto de uma única só função • Proteção OTP básica • Custo do ciclo de vida da ficha 	Um sistema de cartão inteligente substitui uma ficha de uma única função com uma potencial função universal (fixando o acesso da aplicação e da rede) e reduz o custo total da complexidade e do ciclo de vida. O investimento do cartão inteligente pode ter vantagem ao usar o cartão como um crachá inteligente de identificação para o acesso seguro aos edifícios. Os cartões inteligentes são programáveis. Os cartões

Mecanismo de Autenticação	Característica	Valor agregado pelos cartões Inteligentes
		podem ser usados de novo facilmente, suportando uma aproximação mais custo efetiva a emitindo cartões provisórios de acesso. As funções inteligentes novas do cartão podem ser agregadas após a emissão, incorporando suportando melhoras aos sistemas ou às novas aplicações
Leitor Biométrico e senha	<ul style="list-style-type: none"> • Complexa infra-structura de rede (back-end) • Credencial de segurança 	O cartão inteligente prove o armazenamento seguro para o molde biométrico e executa a combinação biométrica no cartão.
Três Fatores autenticação		
Ficha, biométrico, PIN	<ul style="list-style-type: none"> • Credencial de segurança, no servidor ou na estação de trabalho • Infra-estrutura complexa 	Um sistema de cartão inteligente prove menos mecanismos complexos para a autenticação de três fatores quando integrado com a capacidade biométrica de análise do cartão.

Os cartões Inteligentes e a Infra-estrutura IT

Os sistemas operativos de escritórios modernos oferecem um significativo nível de funções aos cartões, com qualquer ajuda incorporada (out-of-the-box) ou pacotes comerciais de softwares. Esta seção descreve as características incorporadas aos sistemas operativos da Microsoft® Windows® e os sistemas operativos de acesso livre da Linux. Também, estão disponíveis à venda sistemas mais sofisticados e com maior capacidade.

Microsoft Windows

A família de sistemas operativos Microsoft Windows incluiu a função de cartão inteligente desde o lançamento do Windows 98 e do NT® 4.0. Esta função permite três tipos de operações:

- Comunicações inteligentes do cartão e do leitor
- Controle de acesso
- Serviços de Web e de E-mail

Cartões Inteligentes e as Comunicações dos leitores

PC/SC

A tecnologia básica para a comunicação entre os ordenadores pessoais e os cartões inteligentes é a PC/SC, definida pelo grupo de trabalho da PC/SC. A PC/SC se define com um Application Program Interfaz (API) que prove aos programadores um sistema de ferramentas estándar para a gerência de leitores de cartões inteligentes e a comunicação entre os leitores e os cartões. A interfaz da PC/SC define uma interfaz estándar para várias operações relacionadas com o cartão inteligente. As mais comuns seriam:

- Enumerar e descrever os leitores de cartões inteligentes adjuntos
- Pedido da informação sobre estados do cartão e do leitor
- Troca de comandos com os cartões

A Microsoft implementou a PC/SC API como parte do Win32® API, o qual é o jogo de ferramentas fundamental para a construção de aplicativos no Windows. Microsoft é também um membro do grupo de trabalho da PC/SC.

O apoio para a implementação da PC/SC da Microsoft se maneja como parte do apoio técnico do sistema operativo do Windows como um todo.

Instalação de leitores de Drivers

A Microsoft utiliza o mesmo método de instalação de drivers de leitor de cartões inteligentes, assim como faz a instalação de outros drivers de hardware no sistema operativo do Windows. Os fabricantes do leitor proporcionam os drivers do dispositivo que são instalados pelo usuário. Depois do driver ser instalado, o leitor é visível com a PC/SC API. Além disso, instalam, previamente, vários leitores recomendados como o Windows 2000, Windows XP, e o Windows 2003.

A complexidade do processo de instalação depende da conexão do hardware. A instalação e a configuração de um leitor de cartões inteligentes unido ao porto USB se realiza de maneira direta. O usuário conecta o leitor ao porto, insere um driver (se for necessário), e segue os avisos. Os

leitores que se conectam ao porto em serie são algo mais difíceis de instalar, tomando em conta que o sistema operativo não pode reconhecer automaticamente o tipo de dispositivo agregado. Entretanto, o processo básico é igual: adjuente o leitor e instale o driver.

A Microsoft tem um programa de registro do Windows para os leitores de cartões inteligentes, que certifica que a Microsoft testou os leitores, verificando que são compatíveis com a implementação dos estándares da PC/SC da Microsoft. A Microsoft recomenda que somente os leitores de cartões inteligentes que tenham sido provados e aprovados possam ser utilizados com os sistemas operativos da Microsoft. Entretanto, a maior parte dos fabricantes de leitores de cartões não aprovados se esforçaram em assegurar que o seu hardware é compatível com os sistemas operativos da Microsoft, sendo, portanto poucos os problemas de incompatibilidade.

CCID

O CCID (Chip Card Interfaz Device ou dispositivo de interfaz do processador do cartão) é um método de comunicação para o leitor de cartões inteligentes que está ganhando renome. A especificação define o protocolo de comunicação estándar para os leitores de cartões inteligentes que se conectam com um computador via USB, permitindo que o mesmo driver do hóspede (host-side driver) se comunique com qualquer leitor de cartões inteligente compatível com CCID. A Microsoft proporciona um driver de CCID através do sistema de actualização do Windows.

Todos os novos leitores de cartão inteligente emitidos devem considerar seriamente o uso de leitores compatíveis com CCID, para reduzir o número de instalações de driver e assegurar-se de que, no futuro, os leitores instalados de cartão inteligente possam ser substituídos de forma fácil e transparente por outro leitor compatível com CCID.

Leitores de cartões inteligentes sem contato

Através da PC/SC e, agora, do CCID, os leitores de contato têm sido muito bem estandarizados e fáceis de integrar. Com a finalização da Revisão 2.0 da especificação PC/SC, que se espera que seja lançada ao mercado em breve, um suporte similar será oferecido aos leitores de cartões inteligentes sem contato. É recomendável que as organizações interessadas em distribuir leitores de cartões inteligentes sem contato utilizem leitores compatíveis com PC/SC.

Comunicação com as aplicações

Depois que um leitor de cartões inteligentes esteja instalado e configurado, um programador de aplicações pode utilizar o PC/SC API para intercambiar comandos com leitor de cartão inteligente. O PC/SC faz um esforço para trata de ocultar as complexidades dos diversos protocolos de comunicação do leitor de cartão mas não pode proporcionar, atualmente, um nível mais elevado de abstração de tipos diferentes de cartão. O API proporciona um canal de comunicações para os comandos do cartão inteligente. A estrutura destes comandos é definida por estándares do ISO, mas o significado destes comandos específicos estão definidos em grande parte pelo fabricante do cartão inteligente individual. Comunicar-se com os cartões inteligentes em um nível de aplicação requer habilidades de programação.

Tomando em conta que a semântica dos comandos está definida pela implementação única de cada cartão inteligente, as aplicações que se desejam operar com diferentes tipos de cartões devem determinar qual é o tipo de cartão e adaptar-se ao sistema de comandos do cartão. Para algumas aplicações, como pagamentos usando a especificação EMV, o sistema de comandos está estandarizado, e a inter-operabilidade é

assegurada pelo vendedor do cartão. Outras aplicações podem alcançar o mesmo efeito usando sistemas operativos de cartões programáveis, tais como Java Card™ ou MULTOS, de tal forma que esses cartões de diferentes vendedores podem ser configurados para responder ao mesmo sistema de comandos da aplicação.

Seleção de Aplicações

A PC/SC proporciona a seleção automática da aplicação. As aplicações se podem registrar-se com a PC/SC, solicitando a notificação quando um tipo particular de cartão inteligentes se insere no leitor. A introdução de um cartão ativa o carregamento de uma aplicação que sabe como utilizar esse cartão.

Autenticação do usuário

O Windows 2000 e o Windows XP proporcionam apoio total para os cartões inteligentes baseados em registro e autenticação, com uma máquina local ou com um servidor do domínio do Windows. O sistema de autenticação de Windows é construído ao redor da PKI, usando um Certificado de autorização Central para publicar os certificados do cartão que associem o usuário da máquina ou do domínio do titular do cartão. Os usuários da Microsoft Internet Explorer e da Outlook® podem também utilizar os certificados nos cartões inteligentes.

Serviço de Web e E-mail

Muitos dos navegadores Web que usam o Windows (tal como Internet Explorer e as famílias populares da Netscape® e de navegadores Mozilla) podem utilizar o cartão inteligente como um símbolo PKCS#11. Um símbolo PKCS#11 mantém certificados e realiza operações chaves privadas. O certificado no cartão inteligente pode executar a autenticação do certificado do cliente a um servidor web, usando os protocolos de SSL/TLS. Além disso, o certificado pode resgitar formas Webs. Não só uma assinatura digital proporciona integridade e autentica o origem do conteúdo da forma, em alguns lugares pode, também, ser uma assinatura digitalmente reconhecida.

Muitos dos correio eletrônico de clientes que usam plataformas Windows, assim como Microsoft Outlook e os correio de clientes integrados a ferramentas web do Netscape e Mozzila, podem usar cartões inteligentes baseados em certificados que registram e encriptam mensagens de correio eletrônico. Mensagens de correio digitalizados e encriptados asseguram que o receptor pode confiar na identidade do emissor – especialmente pois uma mensagem do E-mail pode facilmente ser forjada. A encriptação de correios eletrônicos assegura que o receptor designado possa ler um mensagem e qualquer informação adjunta a este. Devido a que os mensagens de correio atravessam muitos servidores e roteadores, muitas vezes através de redes de acesso público, a encriptação é necessária quando se deseja ter uma comunicação privada.

O Microsoft Outlook apoia a tecnologia estándar de S/MIME para os mensagens digitais de acesso e encriptado do correio eletrônico. O S/MIME usa pares de chaves públicas/particulares nos certificados para poder acessar, encriptar e decriptar operações. O estándar PCKS#11 permite la perspectiva de utilizar uma chave particular armazenada em um cartão inteligente para realizar operações digitais de acesso e descifrado. Se realiza o cifrado usando as chaves públicas armazenadas pelo Outlook na PC do usuário.

Sistema de Encriptação de Arquivo

Os arquivos de sistemas NTFS provistos pelo Windows NT, Windows 2000 e pelo Windows XP oferecem encriptação de arquivos e por endereço, com o fim de proteger o conteúdo dos arquivos (mas não arquivos de nomes). Os arquivos cifrados por contra-senha estão cifrados por uma ou mais contra-senhas públicas que estão armazenadas como os arquivos cifrados. A contra-senha privada dos arquivos utilizada para recuperar a contra-senha cifrada no arquivo esta, normalmente, armazenada em um arquivo local do sistema, mas pode ser armazenada em um cartão inteligente para melhor segurança.

Para o usuário do sistema, a encriptação e descriptação são transparentes. Uma vez que o sistema é configurado, o usuário pode selecionar os arquivos que deveriam ser assegurados. Estes arquivos somente vão abrir quando o cartão inteligente for inserido e, serão inacessíveis quando este for removido. Acessar e escrever nos arquivos cifrados é, geralmente e notavelmente, mais lento que a mesma operação nos arquivos cifrados.

Suporte Oferecido por Diferentes Versões de Windows

Diferentes versões dos sistemas operativos Windows oferecem diversos níveis de suporte para os cartões Inteligentes. A mais recente versão, Windows XP, tem o melhor apoio. Esta prove todos as características descritos acima e vem com drivers incorporados para uma melhor seleção de leitor inteligente. Quase todos os outros fabricantes de leitores de cartões inteligentes provêm drivers para serem utilizados com Windows XP. Windows 2000 também proporciona um amplo suporte para os cartões Inteligentes. A única significativa diferença entre Windows 2000 e Windows XP está em selecionar o leitor do cartão inteligente [provided out-of-the-box](#). Mas, repetimos, outros fabricantes de leitores podem oferecer drivers que funcionem com este sistema operativo.

Windows NT, Windows ME, e o Windows 98 todos oferecem algum nível de suporte para os cartões inteligentes. Proporcionam a maior parte das características descritas acima, mas não proporcionam uma ampla seleção de leitores de drivers. Sumado a isso, dificuldades de menor importância ocorrem com frequência, particularmente durante o processo de instalação. Windows ME e Windows 98 não utilizam o sistema de arquivo NTFS e não proporcionam as características de cifrado do sistema de arquivos, nem proporcionam a opção de conexão do cartão inteligente.

O Windows 95 e o Windows 95SE provêm um suporte não incorporado para os cartões inteligentes. A Microsoft criou um módulo que pudesse ser instalado para executar o cartão inteligente, mas administrar o módulo é difícil. Atualmente, Microsoft deixou o módulo base para cartões inteligentes do Windows 95, e não se sabe por quanto tempo mais o continuaram distribuindo.

Linux

As características dos cartões inteligentes vêm estando disponíveis por vários anos para os sistemas que funcionavam usando o sistema operativo Linux. Não tem nenhum suporte de cartões inteligentes disponível dentro do núcleo da Linux, no entanto as ferramentas de espaço do usuário proporcionam um ambiente de grande alcance para a tecnologia de cartões inteligentes. A maior parte do trabalho realizado pela Smart Card para Linux e outros sistemas operativos da Unix e desenvolvido pelo projeto MUSCLE (para maior informação ver www.musclicard.com)

Uma diferença importante entre o suporte oferecido pela Linux ou pela variedade da Unix e o sistema operativo Windows são as opções. As opções disponíveis de Microsoft são poucas mas se complementam. A Open Source World oferece grandes alternativas, mas muitas das ferramentas de contra-senha, particularmente para implementar uma funcionabilidade de alto nível, de alguma forma são repetidas. Os usuários de funções de segurança do cartão inteligente no Open Source World devem pesquisar para que possam conhecer quais são as opções disponíveis, mas todo esse esforço é quase, geralmente, recompensado com uma solução mais apropriada e mais flexível, para o qual não se requer o pago de permissões.

Cartões Inteligentes e as Comunicações dos leitores

O componente central da infra-estrutura inteligente do cartão da Linux é uma ferramenta chamada PCSC Lite. PCSC Lite executa o PC/SC API definido pelo grupo de trabalho do PC/SC. Esta implementação proporciona as mesmas ferramentas básicas que a implementação da PC/SC em Win32 API da Microsoft.

PCSC Lite

PCSC Lite é uma aplicação de recursos abertos, com uma licença BSD®, que essencialmente dá a cada um a permissão de fazer qualquer coisa que desejem sempre e quando a licença circule pelos usuários, (veja o aviso de direito do autor nos arquivos da PCSC Lite para mais detalhes). A PCSC Lite implementou em várias múltiplas plataformas, incluindo Linux, Solaris™, FreeBSD, NetBSD, OpenBSD, Mac OS® X, HP-UX, e Microsoft Windows. Implementar o PCSS Lite em outros sistemas operativos é sumamente fácil.

O PCSC Lite é estável, rápido, e fácil de usar. De fato, algumas versões do Windows de cartões inteligentes optaram por utilizar PCSC Lite, mais que a implementação da PC/SC, devido a transparência e a flexibilidade da PC/SC Lite.

O suporte gratuito para PCSC Lite está disponível através da lista de correios do projecto, que é também onde acontecem as discussões sobre o desenho e desenvolvimento. As perguntas são respondidas, quase sempre, dentro de uma hora e dentro de um ou dois dias, geralmente pelos programadores da PCSC Lite. A maioria das perguntas de instalação e de desenvolvimento podem ser respondidas buscando os arquivos da lista. Existe um suporte técnico disponível, pago por parte de alguns dos programadores da PCSC Lite; este também se pode conseguir, obtêr das companhias especializadas no Open Source Software, tal como a Red Hat..

A maioria das distribuições da Linux proporcionam pacotes binários de fácil instalação e que configuram automaticamente a PCSC Lite.

Disponibilidade do driver do leitor

Muitos fabricantes dos cartões inteligentes provêm drivers leitores para PC/SC Lite quando estes dispositivos de drivers não estão disponíveis, sendo que algumas vezes existem drivers de vendedores independentes.

Drivers para uma longa seleção de leitores de cartão inteligentes estão disponíveis no www.musclecard.com/drivers.html. Adicionalmente, muitos leitores de cartões inteligentes usam um conjunto de processadores compatíveis, de tal forma que os leitores que não estão listados explicitamente quase sempre funcionam com um drive apropriado. A melhor opção é selecionar um leitor que se conheça para ter um bom produto para PCSC Lite. No entanto, drivers para outros leitores podem ser localizados através do leitor do fabricante na lista do correio eletrônico do PCSC Lite. Se

for necessário, um programador experimentado com as habilidades apropriadas e a apropriada documentação deveria ser capaz de produzir um driver eficiente em 1 ou 2 semanas. Muitos dos fabricantes do PCSC Lite oferecem seus serviços para o desenvolvimento de drivers.

A maioria dos distribuidores da Linux prove drivers pre-pacotes de drivers e, muitas vezes, pre-instalações de drivers para a maior parte dos leitores de cartões inteligentes.

CCID

Existe um driver CCID para la PCSC Lite, em que todos os leitores de cartão inteligente compatíveis com CCID podem trabalhar em todas as plataformas que PCSC Lite suporta.

Autenticação do Usuário

O projeto Muscle prove as ferramentas requeridas para implementar acesso a cartões inteligentes e, qualquer outra autenticação para qualquer sistema operativo que use o sistema conectável de módulos de autenticação (PAM) para autenticarse. Esses sistemas incluem o Linux e a maioria dos sistemas operativos Unix. O Muscle prove o módulo PAM, uma Java Card applet (para o cartão inteligente), ferramentas administrativa e instruções completas para instalar e usar o sistema de autenticação Muscle Card. Os cartões Oberthur AuthentIC e Axalto Cryptoflex são suportes externos, como são todos os outros cartões Inteligentes compatíveis com PKCS#11.

O sistema MuscleCard também proveu ao Windows, um Provedor do Módulo de Serviço Criptográfico para Windows, permitindo que a infraestrutura de cartões inteligentes seja usada com cartões Muscle.

Serviços de Web e E-mail

O projeto MuscleCard proporciona os módulos PKCS#11 permite a autenticação da Web e a assinatura de formulários em todos os mais importantes navegadores Linux, Unix, e Macintosh®. O projeto também proporciona a integração do S/MIME para quase todos os clientes do E-mail que suportem S/MIME. O suporte é proporcionado para qualquer cartão compatível com PKCS#11 ou qualquer cartão Java através do MuscleCard applet.

Além disso, alguns clientes do E-mail, como Kmail, proporcionam PGP/MIME para o registro digital, o cifrado, e o desciframento dos mensagens do correio eletrônico.

Sistemas de Encriptação de Archivos

A pesar de que a Linux include várias ferramentas para o registro de arquivos, nenhum proporciona a conveniência dos arquivos de registro NTFS. No entanto, existem ferramentas que permitem abrir os Cartões Inteligentes em qualquer dos sistemas Linux cifrados.

Uma ferramenta do Linux 2.4, Cryptoloop, transparentemente cifra e descifra uma partição inteira do disco. Configurado em uma forma, Cryptoloop pode cifrar um sistema inteiro, de modo que o sistema inclusive não o elimine sem a apresentação de uma contra-senha apropriada ou de um cartão inteligente. Configurada de outra maneira, Cryptoloop pode proteger um bloco do armazenamento dentro de outra partição insegura. Em qualquer configuração, Cryptoloop tem a vantagem que o nome do arquivo, tamanhos, conteúdo do arquivo, se escondem de usuários desautorizados. Desafortunadamente, a segurança do Cryptoloop vem sendo questionada pelos expertos.

Com a introdução do Linux 2.6, dm_crypt passou a ser a forma recomendada para conseguir uma criptografia transparente de arquivos. Igual que Cryptoloop, dm_crypt opera em partições completas de disco ou em blocos de armazenamento que funcionam como partições. O dm_crypt tem um desempenho mais significativo que o Cryptoloop e dependendo da encriptação escolhida, pode operar tão rápido como um sistema de arquivo decriptografado.

Além das ferramentas transparentes de sistemas de arquivo cifrados, existem ferramentas que fornecem serviços de registro para arquivos individuais ou para grupos de arquivos. Algumas dessas ferramentas protegem nomes de arquivos e tamanhos, ao igual que o conteúdo dos arquivos, e muitas delas se integram com os Cartões Inteligentes. O usuário deve dar os passos para registrar e decriptografar cada arquivo para seu uso. Apesar de que um revisado total dessas ferramentas esta além do alcance destes documentos, um exemplo, KGPG, prove arrastre e verificação de arquivos cifrados e decriptados utilizando uma ferramenta de segurança particular GNUcy Guard.

Soporte Oferecido por Diferentes Variedades de Unix

Quase todas as características de funcionabilidade dos cartões inteligentes descritas neste documento encontram-se disponíveis em qualquer sistema operativo da Unix, incluindo NetBSD, FreeBSD, OpenBSD, Solaris, HP-UX, Mac OS X, IRIX®, e muitos outros. As únicas exceções são Cryptoloop e dm_crypt, nas quais operam somente em Linux..

Para mais informação sobre os cartões inteligentes relacionados com as ferramentas de funções das plataformas que não são as do Windows, use qualquer ferramenta de búsqueda na internet (como Google) e a lista de correio da PCSC Lite.

O Uso de Cartões Inteligentes para Múltiplas Aplicações

As organizações que selecionam os cartões inteligentes para o controle do acesso lógico podem incluir aplicações adicionais ao cartão. Dois avanços recentes tornaram prático o uso de um único cartão inteligente para múltiplas aplicações. Primeiro, a memória do cartão aumentou. Segundo, agora existem sistemas disponíveis de múltiplas aplicações.

A Inclusão de múltiplas aplicações no mesmo cartão oferece as seguintes vantagens:

- Redução de custos. O incremento marginal do custo por acrescentar aplicações ao cartão é significativamente menor que emitir cartões adicionais.
- Conveniência para o possuidor do cartão. É mais conveniente transportar um que varios cartões.
- Eficiência melhorada. Em alguns casos, pode ser possível usar as mesmas credenciais digitais para algumas aplicações, aumentando progressivamente os benefícios dos cartões de múltiplas aplicações.
- Proposta de negócio melhorada. Ao apoiar múltiplas aplicações com um só cartão de identificação inteligente, as organizações podem melhorar seu retorno de inversão realizado em tecnologia de identificação e manter a flexibilidade necessária para o manejo futuro das necessidades organizacionais.

O Uso de Múltiplas Aplicações

Os cartões inteligentes que implementam as aplicações de acesso lógico podem apoiar várias outras aplicações, incluindo as seguintes:

- Aplicações de acesso físico
- Pagamento de aplicações
- Garantir o armazenamento de informação
- Garantir assinaturas digitais
- Aplicações para completar solicitações

Controle de acesso físico

Os cartões inteligentes são idealmente feitos para aplicações de controle de acesso físico, graças as capacidades incorporadas de múltiplas aplicações. Os cartões inteligentes sem contato em particular constituem uma alta tecnologia, para a tecnologia de aproximação 5-KHz amplamente usada, oferecendo conveniência e o meio ambiente e rasgos próprios da tecnologia de aproximação, como a resistência a vândalos e, ao mesmo tempo, acrescenta significativas capacidades de segurança, maior capacidade de armazenamento e apoio de múltiplas aplicações.

A diferença do passado, quando os cartões estavam equipados com menos memória e menos características segurança, o controle de acesso as aplicações de hoje pode agora ser implementado usando diferentes mecanismos. Nos sistemas tradicionais de controle de acesso, um cartão contém um número único que aponta a uma entrada em uma base de dados que grava o nome do possuidor do cartão e os direitos de acesso. Quando esta classe de cartão é apresentada a um leitor, o número é transmitido a um Host, que permitirá ou negará o acesso, baseando-se no número de acesso deste registro na base de dados.

O método tradicional pode seguir sendo usado pelos mesmos cartões inteligentes de hoje, mas uma nova alternativa está disponível. A alternativa é armazenar todas as credenciais do possuidor do cartão de maneira segura no próprio cartão inteligente. Quando o cartão é apresentado ao leitor, este permite o acesso sem necessidade de estar conectado a um Host. Posto que, hoje os cartões inteligentes tenham a maior capacidade de armazenamento, as atuais transações de acesso podem estar escritas no cartão e ser recorridas mais tarde quando o possuidor do cartão apresente o cartão a um leitor em linha.

Outra forma na qual as aplicações de acesso físico podem tomar vantagem da crescente capacidade de armazenamento do cartão é usando informação biométrica como um fator de autenticação. O cartão inteligente pode armazenar de forma segura informação biométrica do possuidor do cartão. Quando o cartão é apresentado a um leitor biométrico, a informação biométrica é extraída do cartão e comparada a do possuidor do cartão para validar a identidade deste. Se a aplicação utiliza uma dos mais poderosos cartões inteligentes com um micro-chip incorporado, a informação biométrica pode ser comparada com a do cartão. Um "match on card" assegura o mais alto nível de privacidade. A informação biométrica nunca deixa o cartão e o cartão pode ser destruído quando o possuidor do cartão deixa uma organização.

O crescente número de organizações tanto do setor público como privado estão adotando os cartões inteligentes para abarcar o acesso físico e lógico usando um só cartão. Por exemplo, a nova identificação do empregado da Microsoft não só abre as portas usando uma interfaz sem contato, esta também apoia um acesso seguro a rede utilizando uma aplicação que reside no contato de um processador incorporado no cartão.

Um cartão inteligente que combina o acesso físico e o lógico permite uma rápida verificação da identidade para poder entrar a um edifício, permite o uso "forte" e uma identificação segura do cartão de identidade (utilizando assinaturas digitais, informação biométrica e tecnologia de contra-senha e PIN), não permite transações falidas e cifra o e-mail. Se uma organização está buscando benefícios como este, como parte de um plano global de segurança da rede, os benefícios podem ser quantificados e incluídos ao plano de negócios para a incorporação da tecnologia de cartões inteligentes.

Atualmente, um dos maiores obstáculos para o desenvolvimento dos mercados de cartões de identificação que abarcam ambos acessos, físicos e lógicos, é a separação historial da segurança física e a segurança de redes. Estas duas funções se manejam, geralmente, por duas seções diferentes em uma organização, cada uma com uma missão, orçamento e infraestrutura tecnológica diferente. Entretanto, como a tecnologia de cartões inteligentes está cada vez mais amplamente disponível em uma variedade de formas, (de contato, sem contato, USB) mais organizações estão desenvolvendo planos de negócios que integrem duas funções de segurança com o propósito de economizar custos e melhorar a segurança da organização amplamente.

Pagos

Os cartões inteligentes permitem transações de pago através da interfaz com contato e sem contato. Como exemplo, a Autoridade do Trânsito da Área Metropolitana de Washington (WMATA) emite aos passageiros um cartão inteligente sem contato, denominado SmarTrip®Card. Os passageiros carregam uma quantidade de dinheiro ao cartão, a seguir usam o cartão para acessar ao Metrô através das cabinas de pago da entrada, que

deduzem automaticamente do cartão o preço da passagem.

O uso da tecnologia de cartão inteligente sem contato foi pioneiro no setor do trânsito, onde a combinação de pago seguro e acesso físico rápido é uma exigência crítica. Os pagos com cartões sem contato estão começando, também, a abarcar o setor de varejo geral. American Express, MasterCard e Visa, todos têm os mesmos programas que usa a tecnologia sem contato, para executar transações seguras de pago com cartão de crédito.

As aplicações de pagamento também podem abarcar um micro-circuito de contato que encaixada no mesmo corpo do cartão, que um micro-circuito sem contato usado para o acesso físico. Atualmente, os micro-circuitos de contato suportam uma variedade larga de aplicações de pagamento, variando desde prêmios eletrônicas, que armazenam o valor monetário, à transações convencionais de crédito e débito. A especificação global da EMV permite que os cartões inteligentes suportem circuitos para transações de crédito e débito, apenas como os cartões magnéticos atuais.

Um cartão inteligente que pretenda suportar, inicialmente, o controle de acesso lógico pode incluir uma aplicação que abarque uma variedade larga de funções de pagamento. A combinação destas funções pode ser um exemplo de um negócio que inclui a tecnologia de cartão inteligente. Para o exemplo, o banco de uma empresa pode fornecer um cartão inteligente incorporado aos empregados, que inclua o programa de pago do banco em um circuito sem contato usado para o acesso físico às facilidades. Os benefícios da empresa seriam os de não ter dois cartões com programas separados, e o banco, além disso, pode incluir algum custo por controlar o programa de acesso. Um outro exemplo (é um que seja executado já em um número de organizações) seria o chamado cartão de campo ou "Campus Card." O cartão de campo é um cartão inteligente universal que pode ser usado como um cartão de identificação (que inclui fotografia) e pode, também, ser usado para pagar pelo alimento e pelos artigos em máquinas de venda, também por portas abertas de dormitórios, para verificar os livros retirados da biblioteca, e pelo pagamento de ligações telefônicas. Geralmente, estes cartões empregam uma variedade de tecnologias, tais como a fita magnética, o código de barras, e um circuito no cartão inteligente, para suportar uma escala de aplicações larga. A maioria das execuções abarcam o controle de acesso físico em combinação com o pagamento e uma variedade de aplicações adicionais, que agregam o valor ao cartão.

Gerência e Armazenamento de Dados Seguros

Os cartões inteligentes estão sendo usados de diversas de formas inovadoras para suportar funções que requerem o armazenamento seguro e portátil da informação sensível e insensível. Como exemplo, os registros médicos podem ser armazenados em um cartão inteligente de modo que somente o possuidor de cartão ou o doutor do possuidor do cartão possa ter acesso aos registros. O acesso a tais registros é protegido tipicamente por um PIN. Similarmente, o Departamento de Defesa emitiu 5.4 milhão cartões comuns de acesso (CAC) ao pessoal militar ativo, ao pessoal selecionado da reserva, aos empregados civis, e um pessoal contratado selecionado. Isso inclui o armazenamento de aplicações de forma segura. O CAC pode armazenar a informação relacionada ao historial médico ou aos outros dados relevantes à missão do possuidor do cartão. Os cartões sem contato usados para sistemas físicos de acesso podem, seguramente, armazenar a informação que recorreu o uso do cartão. Para o exemplo, um cartão sem

contato pode ser usado para gravar, recuperar e examinar os dados de acesso a um edifício em particular (isto é, posição da porta, hora, data). Esta função pode ser controlada pelo cartão ou por uma central.

Acesso a Rede Inalámbrica

Os cartões inteligentes permitem que as organizações controlem o acesso às redes inalámbricas. Os cartões inteligentes podem prover autenticação adequada e universal, abarcar a proteção criptográfica do índice, e facilitar a gerência chave da seção. Adicionalmente, os cartões inteligentes permitem a mobilidade do trabalhador dentro das organizações, aceitando sem problema a re-autenticação e configuração. Com um cartão inteligente, um PIN, e as credenciais apropriadas de acesso, os usuários inalámbricos com exigências de informação extensamente variadas (empregados, clientes, sócios) podem, excepcionalmente, identificar-se às redes ou às aplicações.

Instalação da Aplicação

Quando um cartão inteligente é usado para múltiplas aplicações, estas podem ser carregadas antes ou depois de emitir o cartão. Até recentemente, os procedimentos de instalação da aplicação eram do proprietário. Nos últimos 2 anos, entretanto, a plataforma global criou padrões para personalizar cartões e carregar aplicações. Os padrões da plataforma global permitem que os usuários do cartão combinem vários serviços de forma confidencial.

A instalação da post-emissão requer um pouco mais de esforço do que a instalação da pre-emissão. A informação sobre os cartões emitidos deve estar disponível, incluindo a quantidade de memória disponível no cartão, que chaves ou certificados são necessários que o cartão alcance, e que chaves ou certificados são necessários para instalar novas aplicações. Tal informação está, geralmente, disponível através de um sistema de gerenciamento do ciclo de vida do cartão. A instalação da post-emissão requer também que o cartão possa conectar-se ao Host que fornece a nova nova. Últimamente, instalar aplicações depois que um cartão é emitido confia em ser uma relação entre o emissor da aplicação e do emissor cartão. O emissor do cartão deve ter disponível ou permitir a instalação de uma terceira aplicação ao cartão. Ambos precisam da informação sobre o que está no cartão.

Exemplos de Múltiplas Funções

A tabela 3 mostra exemplos de como os cartões de múltiplas funções estão sendo usados atualmente em muitas execuções. A informação detalhada sobre cada execução pode ser encontrada no apêndice A

Tabela 3: A Implementação do Sistema em Vários Setores

Boeing	<ul style="list-style-type: none">• Crachá de identificação do empregado• Acesso físico• Acesso lógico• Início de uma sessão de Windows 2000 com PIN, PKI e os applet biométricos• Acesso Único a Web• Contra-Senha de bolso "wallet"• Autenticação de VPN• Outras aplicações de planejamento: Encriptação de Dados/e-mail, assinaturas eletrônicas, pagamentos da cafeteria, armazenamento de dados
--------	---

de pessoal, role-based access	
Microsoft	<ul style="list-style-type: none"> • Crachá de identificação do empregado • Acesso físico • Acesso remoto e início de uma sessão às redes incorporadas usando PKI
Rabobank	<ul style="list-style-type: none"> • Acesso lógico às redes e às aplicações usando PKI • Início de uma sessão de Microsoft Windows • Assinaturas Digital
Shell Group	<ul style="list-style-type: none"> • Acesso físico • Acesso do desktop e de rede usando PKI • Acesso e encriptação de documentos e e-mail
Sun Microsystems JavaBadge	<ul style="list-style-type: none"> • Crachá de identificação empregado • Acesso físico • Rede e acesso lógico desktop • Acesso de rede remota • Acesso Único • Encriptação e acesso de E-mail, documentos e transações • Pago E-bolsa
U.S. Department of Defense Common Access Card	<ul style="list-style-type: none"> • Crachás de identificação do empregado • Acesso lógico a redes e desktops usando PKI • Encriptação e acesso a E-mail e documentos • Outras aplicações de planeamento: acesso físico, autenticação biométrica
U.S. Department of State	<ul style="list-style-type: none"> • Crachás de identificação do empregado • Acesso lógico a redes e desktops usando PKI • Encriptação e acesso a E-mail e documentos • Outras aplicações de planeamento: acesso físico, autenticação biométrica

Proposta de Negócios onde se usam cartões Inteligentes e acesso lógico

Muitas empresas estão considerando atualmente o uso de cartões inteligentes para aplicar o acesso lógico seguro. Um estudo³ recente das companhias Fortune 500 dos E.U.A revelou o seguinte:

- Todas as companhias examinadas (100%) estão cientes da tecnologia de cartão inteligente
- Mais de 63% dos executivos entrevistados investigaram ou estão investigando sobre os cartões inteligentes como sistema de segurança
- Mais de 39% das companhias examinadas planeiam usar cartões inteligentes para realçar e fortalecer seus sistemas de segurança nos próximos 3 anos
- Um 30% das companhias está, atualmente, usando ou testando os cartões inteligentes em suas empresas

Para que os cartões inteligentes sejam adotados, o investimento de tecnologia deve ser aplicado de acordo ao exemplo apropriado do negócio, que requer a consideração de benefícios tangíveis e intangíveis.

Benefícios Intangíveis

Os negócios investem em tecnologia forte de autenticação por duas razões principais:

Regulatory compliance

Posicionamento estratégico

← - - - Formatted: Bullets and Numbering

Regulatory Compliance

Os negócios estão requerindo cada vez mais este sistema, para realçar seus processos de autenticação para cumprir com as exigências externas. Tais exigências externas incluem novas legislações ou regulamentações (por exemplo, HIPAA, Sarbanes-Oxley) e outros padrões do governo ou da indústria. Nesses casos, os negócios são requeridos tipicamente para demonstrar que se encontram com determinados padrões prescritos. Uma falha destes padrões pode resultar em penalidades financeiras significativas. A exigência para promover sistemas de informação que oferecem uma autenticação mais forte é vista geralmente pela gerência *sênior* como o custo de fazer o negócio em um setor ou em um mercado dado. Além disso, as violações de privacidade podem resultar em penalidades significativas.

Posicionamento Estratégico

Os cartões inteligentes são peça chave na segurança de uma empresa. Com respeito a isso, não são diferentes aos directory servers, VPNs, sistemas de detecção de intrusos, ou firewalls. Os negócios estão começando a reconhecê-lo para manter uma vantagem competitiva, e assim assegurar-se de que seus recursos intelectuais estejam bem defendidos. Determinados negócios estabeleceram um Chefe de Segurança (CSO) para assegurar-se de que os interesses da mesma fossem dirigidos de uma forma holística. Para ser eficaz, a posição do CSO obedece somente ao CEO. Os cartões inteligentes são atrativos dentro de tal ambiente, desde que atuem como uma ponte entre os domínios físicos e lógicos da segurança.

³ "Fortune 500 Companies' Preference for Corporate Security Applications," Frost & Sullivan, Feb. 17, 2003.

Benefícios Tangíveis

É altamente provável que uma organização que esteja considerando o uso de cartões inteligentes herdará uma infra-estrutura, composta tipicamente pelo seguinte:

- Contra-senha de usuário baseada na autenticação local
- Símbolos OTP para um acesso remoto seguro com a finalidade de proteger os bens.
- Uma infra-estrutura de crachás de identificação com suporte a um sistema de controle físico.

As organizações normalmente consideram um conjunto de acesso físico e lógico com base nos cartões inteligentes. Esses cartões incluem contato interfacial para reforçar o acesso aos edifícios e contato interfacial para apoiar o acesso lógico. Historicamente esses dois componentes têm sido separados fisicamente mas existe uma tendência ao crescimento para que as duas funções coexistam em um chip com interface dupla com processamento e capacidade de armazenamento de dados significativo.

Entre os benefícios de tal sistema estão os seguintes:

- Uso administrativo simplificado
- A eliminação dos símbolos OTP e toda a infra-estrutura associada (e.x. servidores)
- Aumento da produtividade de uso

Uso Administrativo Simplificado para el Usuario

Gastos significativos estão associados com a manutenção dos sistemas tradicionais de acesso a sistemas mediante contra-senha. Por exemplo, o Grupo Aberdeen descobriu que o custo de configuração e manutenção do sistema de acesso a sistemas mediante contra-senhas para as pequenas empresas varia dos \$100 a \$150 ao ano por usuário. Custos para uma mediana empresa estão ao redor de \$200, e uma companhia gasta uma média de \$300 a \$350 ao ano por usuário..

De fato, não é comum que os departamentos IT instalem um cargo interno por tomar conta da manutenção de contra-senhas. A administração do sistema de cartões inteligentes oferece um auto-serviço, vantagem que reduz os gastos gerais na manutenção do sistema de contra-senhas. Enquanto informações confidenciais (como os PINs) ainda precisam ser administradas, o sistema de cartões inteligentes inclui um controle do sistema de usuários que pode diminuir de maneira significativa os gastos com manutenção dessa informação confidencial.

Eliminação das Fichas OTP

As fichas OTP são caras de adquirir e controlar e têm um alto índice de erros. O custo de uma ficha OTP pode ser aproximadamente de \$100 ao ano por usuário. Os cartões Inteligentes oferecem uma função equivalente mas a um custo reduzido de posse.

Redução da Infra-estrutura global

Combinar o acesso lógico e físico a um símbolo individual oferece às organizações a oportunidade de eliminar a tecnologia redundante.

Tipicamente, o sistema de cartões inteligentes são vistos como uma melhora, ao invés de uma substituição atualizada do sistema de acesso físico OTP.

Aumento da Produtividade

A introdução dos cartões inteligentes normalmente coincide com outras iniciativas de simplificar o fluxo pessoal dos negócios, de tal forma que gere o aumento da produtividade e da eficiência dos empregados. Uma autenticação mais forte normalmente aumentará a eficiência dos diferentes serviços tanto internos como externos, gerando uma melhoria que pode ser medida através dos lucros. Tais melhorias podem ser multiplicadas se negociadas entre sócios que utilizem o mesmo tipo de "software" interoperáveis.

Investimentos

Os cartões inteligentes e cartões inteligentes associados a sistemas representam um investimento. O nível da inversão vai depender do número de fatores implicados, incluindo à organização da infra-estrutura e da autenticação das técnicas implementadas. Os gastos descritos abaixo são fundamentais para adquirir e acessar à informação de autenticação do sistema de cartões inteligentes.

O Cartão Inteligente. Os Cartões inteligentes são mais caros por si mesmos que os crachás de identificação, tendo um custo por cartão de \$5 a \$10.

Os Leitores de Cartão Inteligente. Não é estranho que os computadores sejam entregues com cartões inteligentes já incorporados às mesmas. Para sistemas legados, um leitor de cartão inteligente externo típico ligado ao porto USB de um computador, pode ser adquirido por aproximadamente \$15 (em volume). A sistema USB do cartão inteligente pode conectar-se diretamente no porto do USB de um computador, não requerendo nenhum investimento adicional da ferramenta.

Middleware. Para permitir o processo de autenticação do cartão inteligente, o middleware deve ser instalado na estação de trabalho de cada usuário. Os custos variam de \$2 a \$10 por lugar, dependendo da técnica de autenticação que estiver sendo executada.

Sistema de Gerenciamento do Cartão Inteligente. Um sistema de gerenciamento do cartão inteligente abarca a emissão e o ciclo de vida dos cartões e das credenciais armazenadas neles. Os sistemas variam na potencialidade e na complexidade dependendo da técnica de autenticação que abarcam, e podem variar de \$5 a \$50 por usuário.

Infra-estrutura da Técnica de Autenticação. Quando usados para o acesso lógico, os cartões inteligentes executam uma seletiva técnica de autenticação de uma organização, ou uma combinação selecionada das técnicas. As técnicas podem incluir contra-senhas de vários tipos, chaves de autenticação simétricas, chaves de autenticação assimétricas e dados biométricos. O custo da infra-estrutura para incluir a técnica escolhida de autenticação necessita ser considerado. Os cartões inteligentes fornecem uma vantagem. Sua habilidade de incluir várias técnicas de autenticação em um único cartão de identificação permite que uma organização execute a autenticação requerida para encontrar-se com as exigências de segurança da organização. A facilidade de agregar aplicações aos cartões inteligentes depois de serem emitidos permite que as organizações comecem a usar cartões inteligentes para o simples armazenamento da contra-senha, assim

como técnicas mais fortes de autenticação, se for desejado, sem reinvestir nos cartões e nos leitores.

Outros Custos do Projeto. Implementar um novo sistema de gerência de identidade pode ser um projeto a grande escala. O investimento será requerido no processo de re-estruturação do negócio, treinamento do usuário, e na assistência, assim como o gerenciamento inicial da configuração do sistema e da distribuição do projeto.

A tabela 4 sumaria os benefícios, as economias, e os custos potenciais chave que devem ser considerados ao executar um sistema de acesso lógico baseado em cartões inteligentes.

Table 4: Smart Card Logical Access Systems – Savings and Costs

Benefícios e economias chaves	Custos
<ul style="list-style-type: none"> • Gerência simplificada da contra-senha do usuário <ul style="list-style-type: none"> - abaxe custos da sustentação -conveniência aumentada do usuário • Custos de eliminação de símbolos OTP • Redução dos custos de infra-estrutura combinando várias funções em um único crachá de identificação inteligente • Conformidade legislative e reguladora (Legislative and regulatory compliance) • Melhoria na produtividade do usuário e custos de operação reduzidos <ul style="list-style-type: none"> - acesso mais fácil aos recursos da rede de trabalho - Melhorias dos processos (por exemplo, documento de acesso) • Risco reduzido de ruptura da segurança e de seus custos (por exemplo, financeiro, produtividade, vendas, posição do mercado, exposição legal) • Abilidade de migrar às técnicas mais fortes ou diferentes de autenticação sem re-investir nos cartões e nos leitores. 	<ul style="list-style-type: none"> • Custo do cartão inteligente • Custo do leitor de cartão inteligente (se usado em forma de cartão) • Cliente middleware • Sistema de gerenciamento do cartão inteligente • Custos de implementar uma infra-estrutura de autenticação escolhida (e.x., dados biométricos, PKI, chaves simétricas) • Custos de projeto IT: gerência do projeto, treinamento do usuário, re-estruturação do negócio, configuração do sistema e distribuição.

Conclusões

Cada dia uma notícia destaca a importância da segurança nas redes corporativas, que é, frequentemente, quebrantada; sistemas de informação são acessados por indivíduos não autorizados e as identidades são roubadas e usadas para realizar transações fraudulentas. Como resultado disso, tanto os negócios como o governo estão avaliando ou implementando novos sistemas de administração/gerência de identidades para prover acesso lógico mais seguro.

Para conseguir um sistema forte de autenticação para o acesso se requer o uso de múltiplos fatores de autenticação. A tecnologia de cartão inteligente, regularmente, usada em conjunto com um PIN para abrir o cartão, está, cada vez mais, sendo usada para oferecer um importante, segundo ou terceiro, fator de autenticação que faz o acesso lógico mais seguro.

A tecnologia de cartão inteligente está disponível em múltiplas formas (cartão plástico, aparelho USB ou como um circuito SIM de um telefone celular) e apoia todas as técnicas de autenticação comumente usadas para assegurar o acesso lógico: cartões inteligentes, dispositivos com seguro, sistemas anti-roubo fáceis de usar. Os cartões inteligentes podem apoiar a múltiplas aplicações permitindo a um só cartão de identificação realizar múltiplas funções. Por exemplo, o mesmo cartão de identificação inteligente pode permitir a um indivíduo entrar a um edifício, acessar a rede interna de informação, assinar documentos, encriptar o correio eletrônico, fazer transações e pagar seu almoço na lanchonete da organização, tudo isso de maneira segura. Esta flexibilidade ajuda à organização a desenvolver um forte sistema de controle de acesso em base a cartões inteligentes.

A Smart Card Alliance incita as organizações que estão avaliando introduzir um melhor sistema de identificação e sistemas de controle de acesso lógico a implementar a tecnologia de cartão inteligente. A tecnologia de cartão inteligente prove a base para a privacidade, a confiança e a segurança em aplicações lógicas de acesso. A combinação da tecnologia de cartão inteligente e a autenticação universal melhora a segurança, realça a conveniência do usuário e entrega benefícios poderosos ao negócio.

Para mais informação sobre os cartões inteligentes e a função que têm na identificação segura e em outras funções, por favor visite a Smart Card Alliance em este sitio Web www.smartcardalliance.org ou fale conosco diretamente chamando ao 1-800-556-6828.

Referências e Fontes

"2004 E-Crime Watch™ Survey Shows Significant Increase in Electronic Crimes," CSO Magazine survey conducted in cooperation with the United States Secret Service and Carnegie Mellon University Software Engineering Institute's CERT® Coordination Center, May 25, 2004
(http://www.csoonline.com/releases/052004129_release.html)

"Ask the Analyst: Passwords Are Gobbling Up your Profits," Jim Hurley, Aberdeen Group, May 1, 2003

"The Boeing Company Chooses Siemens to Enhance Physical and Information Security with Identity Management System," Siemens and Boeing press release, Sept. 8, 2003,
http://www.siemens.com/index.jsp?sdc_p=cs4uo1093899pnfilm

"Boeing SecureBadge Program," Sharon Lindley, SecureBadge Program Director, Boeing, Smart Card Alliance Annual Conference presentation, Oct. 16, 2003

Department of Defense Personal Identity Protection (PIP) Program, DoD Directive Number 1000.25, July 19, 2004
(<http://www.dtic.mil/whs/directives/corres/html2/d100025x.htm>)

Electronic Authentication Partnership (EAP), <http://www.eapartnership.org>

"Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology," NIST Computer Security Division, NIST Special Publication 800-63, Version 1.0, June 2004

"Endpoint Security Management: Maximizing Best of Breed," IDC report, March 4, 2004

"Fortune 500 Companies' Preference for Corporate Security Applications," Frost & Sullivan, Feb. 17, 2003

"FTC Releases Survey of Identity Theft in U.S. 27.3 Million Victims in Past 5 Years, Billions in Losses for Businesses and Consumers," FTC press release, Sept. 3, 2003, <http://www.ftc.gov/opa/2003/09/idtheft.htm>

Global Platform (<http://www.globalplatform.org>). Industry association that is creating and advancing interoperable technical specifications for smart cards, acceptance devices and systems infrastructure.

"Government Smart Card Handbook," February 2004, available at <http://www.smartcardalliance.org>

"HIPAA Compliance and Smart Cards: Solutions to Privacy and Security Requirements," Smart Card Alliance report, September 2003, available at <http://www.smartcardalliance.org>

Initiative for Open Authentication (OATH), <http://www.openauthentication.org>

International Civil Aviation Organization (ICAO) Machine Readable Travel Documents (MRTD), <http://www.icao.int/mrtd/Home/Index.cfm>

MUSCLE Project (<http://www.musclecard.com>). MUSCLE is a project to coordinate the development of smart cards and applications under Linux.

NIST Personal Identity Verification (PIV) Project (<http://csrc.nist.gov/piv-project/index.html>)

Liberty Alliance, <http://www.projectliberty.org>

"One Card Fits All," Boardroom Minutes: Technology Intelligence for Business Executives, available at <http://www.sun.com/software/sunone/boardroom/newsletter/0603solutions.html>

OpenCard Consortium, <http://www.opencard.org>

Open Security Exchange (OSE), <http://www.opensecurityexchange.com>

PC/SC Workgroup (<http://www.pcscworkgroup.com>). Industry group who developed the PC/SC specification, which defines how to integrate smart card readers and smart cards with the computing environment and how to allow multiple applications to share smart card devices.

"“phishing” Victims Likely Will Suffer Identity Theft Fraud," Gartner press release, May 14, 2004, http://www3.gartner.com/5_about/press_releases/asset_71087_11.jsp

"Privacy and Secure Identification Systems: The Role of Smart Cards as a Privacy-Enabling Technology," Smart Card Alliance white paper, February 2003, available at <http://www.smartcardalliance.org>

"Secure Identification Systems: Building a Chain of Trust," Smart Card Alliance report, March 2004, available at <http://www.smartcardalliance.org>

"Securing the Enterprise," Albert Leung, Group Marketing Manager, Java Card Technology, Sun Microsystems, Smart Card Alliance Annual Conference presentation, October 16, 2003

Smart Card Alliance Smart Card Reader Catalog, available at http://www.smartcardalliance.org/industry_info/catalog.cfm

"Smart Card Case Studies and Implementation Profiles," Smart Card Alliance report, December 2003, available at <http://www.smartcardalliance.org>

"Smart Card Deployment at Microsoft," Microsoft white paper, March 11, 2004, available at <http://www.microsoft.com/technet/itsolutions/msit/security/smartcard.msp>

USB Implementer's Forum, <http://www.usb.org>

"Using Smart Cards for Secure Physical Access," Smart Card Alliance report, July 2003, available at <http://www.smartcardalliance.org>

Reconhecimentos

This report was developed by the Smart Card Alliance to discuss the issues with authenticating individuals for logical access and to define the benefits that smart card technology provides. Publication of this document by the Smart Card Alliance does not imply the endorsement of any of the member organizations of the Alliance.

The Smart Card Alliance wishes to thank the Secure Personal ID Task Force members for their contributions. Participants from 22 organizations were involved in the development of this report including: ActivCard, AOS-Hagenuk, Axalto, CardLogix, Datakey, Gemplus, Honeywell Access Systems (OmniTek), IBM, Identix, Litronic/SAFLink, Lockheed Martin, MartSoft Corporation, Northrop Grumman Information Technology, OTI America, SCM Microsystems, Smart Commerce, Inc., Sun Microsystems, U.S. Department of Defense, VeriFone, VeriSign, Visa USA, XTec, Incorporated.

Special thanks go to the individuals who wrote, reviewed and edited this report.

David Asay, IBM

David Berman, VeriSign

Kirk Brafford, Litronic/SAFLink

Yuh-Ning Chen, Ph.D., MartSoft Corporation

Michael Davis, Honeywell Access Systems (OmniTek)

Patrice Erickson, Identix

Nick Hislop, Gemplus

Mansour Karimzadeh, Smart Commerce, Inc.

Colleen Kulhanek, Datakey

Kevin Kozlowski, XTec Inc.

Albert Leung, Sun Microsystems

Mark McGovern, Lockheed Martin

John McKeon, IBM

Cathy Medich, Consultant & Task Force Chair

Yahya Mehdizadeh, Axalto

Bob Merkert, SCM Microsystems

Neville Pattinson, Axalto

Dwayne Pfeiffer, Northrop Grumman Information Technology

Bruce Ross, CardLogix

Nick Stoner, Lockheed Martin

Shawn Willden, IBM

Direitos do Autor

Copyright 2004 Smart Card Alliance, Inc. All rights reserved.

Marca Registrada

All registered trademarks, trademarks, or service marks are the property of their respective owners.

Apple, Macintosh and Mac OS are trademarks of Apple Computer, Inc., registered in the U.S. and other countries.

BSD is a registered trademark of Berkeley Software Design, Inc.

CosmopolIC is a trademark of Oberthur.

Entelligence is a trademark of Entrust.

IRIX is a registered trademark of Silicon Graphics, Inc., in the U.S. and/or other countries.

Mediametric is a trademark of XTec, Incorporated.

Microsoft, Windows, Windows NT, Win32, Outlook are either registered trademarks or trademarks of Microsoft Corporation in the U.S. and/or other countries.

MIFARE is a trademark of Philips Semiconductors.

Netscape is a registered trademark of Netscape Communications.

OS/2 is a registered trademark of IBM Corporation.

SecurID is a registered trademark of RSA Security Inc. in the United States and/or other countries.

S/KEY is a registered trademark of Bell Communications Research.

SmarTrip is a registered trademark of WMATA.

Sun, Sun Microsystems, Sun Ray, Java, Java Card and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

Unix is a registered trademark of The Open Group.

Appendix A: Definition of Terms and Acronyms

API

Application programming interfaz. A formal specification of a collection of procedures and functions available to an application programmer. These specifications describe the available commands, the arguments (or parameters) that must be provided when calling the command, and the types of return values when the command execution is completed.

Asymmetric keys

Two related keys, a public key and a private key, that are used to perform complementary operations, such as encryption and decryption or signature generation and signature verification.

Biometric

Automated methods of identifying or authenticating the identity of a living person based on unique physiological or behavioral characteristics.

Biometric template

The stored record of an individual's biometric features. Typically, a "livescan" of an individual's biometric attributes is translated through a specific algorithm into a digital record that can be stored in a database or on a smart card. The formatted digital record used to store the biometric attributes is generally referred to as the biometric template

BSD

A version of Unix developed at the University of California at Berkeley.

Certificate authority (CA)

A component of the Public Key Infrastructure that is responsible for issuing and revoking digital certificates. Digital certificates may contain the public key or information pertinent to the public key.

Checksum

A computed value that depends on the contents of a message. The checksum is transmitted with the message. The receiving party can then recompute the checksum to verify that the message was not corrupted during transmission.

Cleartext

Data or information that is not encrypted.

Chip

Electronic component that performs logic, processing, and/or memory functions.

Contact smart card

A smart card that connects to the reading device through direct physical contact between the smart card chip and the smart card reader.

Contactless smart card

A smart card whose chip communicates with the reader using RF and does not require physical contact with the card reader.

DES

Data Encryption Standard.

DSA

Digital Signature Algorithm.

Dual interfaz card

A smart card that has a single smart card chip with two interfaz – a contact and a contactless interfaz – using shared memory and chip resources.

EMV

Europay MasterCard Visa. Specifications developed by Europay, MasterCard, and Visa that define a set of requirements to ensure interoperability between payment chip cards and terminals.

Gramm-Leach-Bliley

The Financial Services Modernization Act of 1999 (also known as the Gramm-Leach-Bliley Act), enacted to facilitate affiliation among banks, securities firms, and insurance companies. The Act includes provisions to protect consumers' personal financial information held by financial institutions.

GSC-IS

Government Smart Card Interoperability Specification. The GSC-IS was defined to provide the ability to develop secure identification smart cards that can operate across multiple government agencies or among federal, state, and local governments and provides solutions to a number of interoperability issues associated with contact smart card technology implementation.

GSM

Global System for Mobile Communications

Hash algorithm

A software algorithm that computes a value (hash) from a particular data unit in a manner that enables detection of intentional/unauthorized or unintentional/accidental data modification by the recipient of the data.

HIPAA

Health Insurance Portability and Accountability Act of 1996. HIPAA was passed to protect health insurance coverage for workers and their families and to encourage the development of a health information system by establishing standards and requirements for the secure electronic transmission of certain health information. HIPAA mandates that the design and implementation of the electronic systems guarantee the privacy and security of patient information gathered as part of providing health care.

Hybrid card

An ID card that contains two smart card chips – both contact and contactless chips – that are not interconnected.

ICAO MRTD

International Civil Aviation Organization Machine Readable Travel Documents. ICAO establishes international standards for travel documents. An MRTD is an international travel document (e.g., a passport or visa) containing eye- and machine-readable data. ICAO Document 9303 is the international standard for MRTDs.

Integrated circuit

See chip.

ISO

International Organization for Standardization.

ISO/IEC 14443

ISO/IEC standard "Identification Cards - Contactless Integrated Circuit(s) Cards - Proximity Cards."

ISO/IEC 7816

ISO/IEC standard for integrated circuit cards with contacts.

Logical access

Access to online or networked resources (e.g., networks, files, computers, databases).

Man-in-the-middle attack

An attack on an authentication protocol in which the attacker is positioned between the individual seeking authentication and the system verifying the authentication. In this attack, the attacker attempts to intercept and alter data traveling between the parties.

MCU

See microcontroller.

MD5

One of the most popular hashing algorithms, developed by Professor Ronald L. Rivest of MIT, which produces a 128-bit hash from any input.

Microcontroller (MCU)

A highly integrated computer chip that contains all the components comprising a controller. Typically this includes a CPU, RAM, some form of ROM, I/O ports, and timers. Unlike a general purpose computer, a microcontroller is designed to operate in a restricted environment.

Microsoft Crypto API

The Microsoft security framework that developers use to implement security functions for applications that run on Microsoft Windows.

Multi-application card

A smart card ID that runs multiple applications – for example, physical access, logical access, data storage, and electronic purse – using a single card.

NIST

National Institute of Standards and Technology.

Non-repudiation

The ability to ensure and have evidence that a specific action occurred in an electronic transaction (e.g., that a message originator cannot deny sending a message or that a party in a transaction cannot deny the authenticity of their signature).

NTFS

New Technology File System. Windows proprietary file system.

OTP

One-time passwords are passwords that are used once and then discarded. Each time the user authenticates to a system, a different password is used, after which that password is no longer valid. The password is computed either by software on the logon computer or OTP hardware tokens in the user's possession that are coordinated through a trusted system.

PC

Personal computer.

PC/SC

Personal Computer/Smart Card. The PC/SC specification defines how to integrate smart card readers and smart cards with the computing environment and how to allow multiple applications to share smart card devices.

PCSC Lite

Personal Computer/Smart Card Lite. PCSC Lite is open source software that implements the PC/SC specification for Linux.

PGP/MIME

Pretty Good Privacy/Multipurpose Internet Mail Extensions. A protocol for exchanging digitally signed and/or encrypted mail.

Physical access

Access to physical facilities (e.g., buildings, rooms, airports, warehouses).

PIN

Personal Identification Number. A numeric code that is associated with an ID card and that adds a second factor of authentication to the identity verification process.

Public (asymmetric) key cryptography

A type of cryptography that uses a pair of mathematically related cryptographic keys. The public key can be made available to anyone and can encrypt information or verify a digital signature. The private key is kept secret by its holder and can decrypt information or generate a digital signature.

PKI

Public Key Infrastructure. The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a certificate-based public key cryptographic system. Further, a communications infrastructure that allows users to exchange money and data over the Internet in a secure environment. There are four basic components to the PKI: the certificate authority (CA) responsible for issuing and verifying digital certificates, the registration authority (RA) which provides verification to the CA prior to issuance of digital certificates, one or multiple directories to hold certificates (with public keys), and a system for managing the certificates. Also included in a PKI are the certificate policies and agreements among parties that document the operating rules, procedural policies, and liabilities of the parties operating within the PKI.

PKCS #11

Public Key Cryptography Standard #11. This standard defines the interfaz for cryptography operations with hardware tokens.

Private key

The secret part of an asymmetric key pair that is used to create digital signatures and, depending upon the algorithm, to decrypt messages or files encrypted (for confidentiality) with the corresponding public key.

Public key

The public part of an asymmetric key pair that is used to verify signatures created with its corresponding private key. Depending on the algorithm, public keys are also used to encrypt messages or files that can then be decrypted with the corresponding private key.

Public key certificate

A digital document that is issued and digitally signed by the private key of a CA and that binds the name of a subscriber to a public key.

RF

Radio frequency.

RFID

Radio frequency identification

RSA

Refers to public/private key encryption technology that uses an algorithm developed by Ron Rivest, Adi Shamir, and Leonard Adleman and that is owned and licensed by RSA Security.

Sarbanes-Oxley

The Sarbanes-Oxley Act of 2002, which introduced changes to regulations that apply to financial practice and corporate governance for public companies. The Act introduced new rules that were intended "to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws."

Secure Hash Algorithm (SHA)

One of the most popular hashing algorithms, designed for use with the Digital Signature Standard by the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA). SHA-1 produces a 160-bit hash.

Seed

A random sequence of bits that is used in a cryptographic algorithm as the input to generate other, longer pseudo-random bit sequences.

SIM

Subscriber Identity Module. A SIM is the smart card that is included in GSM (Global System for Mobile Communications) mobile phones. SIMs are configured with information essential to authenticating a GSM mobile phone, thus allowing a phone to receive service whenever the phone is within coverage of a suitable network.

Smart card

A device that includes an embedded chip that can be either a microcontroller with internal memory or a memory chip alone. The card connects to a reader with direct physical contact or with a remote contactless electromagnetic interfaz. With an embedded microcontroller, smart cards have the unique ability to store large amounts of data, carry out their own on-card functions (e.g., encryption and digital signatures) and interact intelligently with a smart card reader. Smart cards are available in a variety of form factors, including plastic cards, SIMs, and USB-based tokens.

Smart ID card

An identification card that is a smart card.

S/MIME

Secure Multipurpose Internet Mail Extensions. A protocol for exchanging digitally signed and/or encrypted mail.

Sniffing

The act of auditing or watching computer network traffic. Hackers may use sniffing programs to capture data that is being communicated on a network (e.g., usernames and passwords).

SSL

Secure Sockets Layer. SSL is a protocol used to transmit information on the Internet in encrypted form. SSL also ensures that the transmitted information is only accessible by the server that was intended to receive the information.

Strong authentication

The use of two or three factors of authentication to prove an individual's identity. Factors would include some combination of something you know (a password or personal identification number that only you know), something you have (a physical item or token in your possession) and something you

are (a unique physical quality or behavior that differentiates you from all other individuals).

Symmetric keys

Keys that are used for symmetric (secret) key cryptography. In a symmetric cryptographic system, the same secret key is used to perform both the cryptographic operation and its inverse (for example to encrypt and decrypt, or to create a message authentication code and to verify the code).

TLS

Transport Layer Security protocol. The TLS protocol provides communications security over the Internet.

Token

A hardware security device that contains a user's identity credentials and the security keys required to use the credential, authenticate the individual, and/or perform secure transactions. This may include the individual's private key(s), public key certificate, and optionally other certificates.

3DES

Triple DES.

USB

Universal Serial Bus.

VPN

Virtual private network.