Nota de aplicação

Usos do produto Atmel CryptoAuthentication

Atmel ATSHA204

Abstrato

As empresas estão continuamente procurando maneiras de proteger a propriedade usando várias implementações de segurança; no entanto, o custo da implementação da segurança pode afastar as empresas de soluções de hardware eficazes para soluções de software menos seguras. Com a introdução do dispositivo Atmel® ATSHA204 CryptoAuthentication™ , a segurança de hardware acessível está prontamente disponível e fornece proteção excepcional.

Visão geral

O ATSHA204 é um dispositivo excepcional que permite soluções para inúmeros problemas em muitos setores. Descritos neste documento estão os casos de uso que fornecem breves descrições dos possíveis aplicativos ATSHA204 e como esses aplicativos podem ser implementados.

1. Autenticação de acessórios

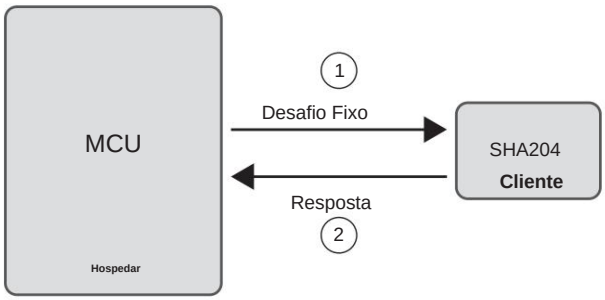
O processo de autenticação de resposta de desafio fixo abaixo pode ser usado para vários casos de uso. Para fins de explicação, a Resposta de Desafio Fixa é usada em um aplicativo acessório.

A ATSHA204 CryptoAuthentication pode ser usada para autenticar um acessório. Para fazer a autenticação, o ATSHA204 deve estar embutido no acessório (Cliente).

O processo de autenticação usa um par desafio-resposta selecionado de um conjunto de pares desafio-resposta. Antes de usar o acessório, um desafio é enviado para ATSHA204 no Cliente. O Cliente então calcula a resposta e envia a resposta ao Host. Ao receber a resposta, o Host a compara com a resposta esperada. Se as respostas coincidirem, diz-se que o Cliente é autêntico.

Ao usar esta configuração, apenas acessórios autênticos podem ser usados pelo sistema. O processo de autenticação do acessório é ilustrado na Figura 1-1.

Figura 1-1. Resposta de Desafio Fixa



As possíveis aplicações estão listadas abaixo:

- ÿ Dispositivos móveis — autenticando a bateria
- ÿ Autenticação de equipamentos médicos
- ÿ Acessórios do dispositivo, como fones de ouvido, alto-falantes, docking station, carregadores, etc.

2. Autenticação de consumíveis

O processo de autenticação Random Challenge Response abaixo pode ser usado para uma infinidade de casos de uso. Para fins de explicação, a Resposta de Desafio Aleatório é usada em um aplicativo consumível.

Ao incorporar o dispositivo ATSHA204 em um consumível (Cliente) e enviar um desafio do sistema (Host), as empresas podem garantir que apenas consumíveis autênticos sejam usados em seus sistemas.

Neste esquema, um desafio aleatório é usado para autenticar o produto consumível. Antes de usar o consumível, o Host recebe um desafio aleatório ao Cliente. O Cliente então calcula a resposta e envia a resposta ao Host. Ao receber a resposta, o Host a compara com a resposta esperada.

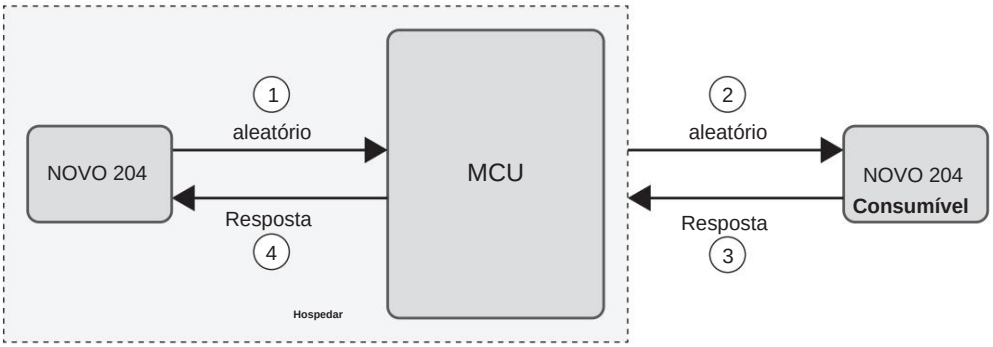
O ATSHA204 possui um recurso especial para limitar a quantidade de uso do consumível conectado ao sistema. O ATSHA204 possui uma chave especial que pode ser usada apenas para uso limitado. A quantidade de uso da chave diminui cada vez que a chave é usada para realizar a autenticação. Após um máximo de 128 utilizações, a chave é permanentemente desativada. Qualquer uso adicional dessa chave retornará um erro. Se forem necessárias mais de 128 contagens, existe um método para encadear os slots.
Consulte a nota de aplicação, “Encadeamento Atmel ATSHA204 de Chaves para Consumo”.

Para aumentar o nível de segurança, um esquema de chave diversificada pode ser usado. Nesse esquema, cada ATSHA204 teria uma chave única que é diversificada com base em seu número de série. Se um acessório for comprometido, isso não afetará outro acessório porque cada acessório possui uma chave exclusiva.

Um nível adicional de segurança pode ser adicionado ao sistema usando outro dispositivo ATSHA204 no host. O ATSHA204 mantém as chaves secretas no hardware em vez de incorporá-las ao código do microprocessador Host. Isso torna as chaves irrecuperáveis para hackers que tentam contornar o sistema.

A Figura 2-1 ilustra um exemplo do uso do dispositivo ATSHA204 para validar consumíveis.

Figura 2-1. Resposta de desafio aleatório



O uso do número de série para implementar um esquema de diversificação de chaves é recomendado para limitar os efeitos adversos se uma das chaves for comprometida por processos de controle falhos ou espionagem corporativa. Ao usar uma chave diversificada, a fonte de comprometimento pode ser isolada e um remédio pode ser implementado muito mais rapidamente.

As aplicações possíveis para esta configuração são: ÿ

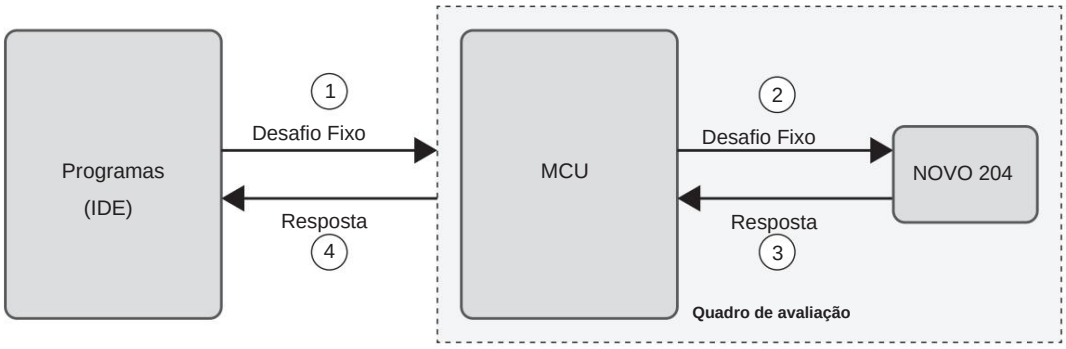
Impressoras — autenticando o cartucho. ÿ Purificação

do ar — autenticando o filtro.

3. Anticlonagem/antipirataria do sistema

ATSHA204 CryptoAuthentication fornece um método excepcional que impede que terceiros criem clones de placa. Para implementar, a placa deve ser incorporada com seu próprio dispositivo ATSHA204. O Ambiente de Desenvolvimento Integrado (IDE) seria então programado para desafiar o conselho antes de permitir o acesso do desenvolvedor a ele. Os falsificadores não serão capazes de replicar todas as possíveis ocorrências de desafio e resposta que podem ser tratadas por uma placa contendo um dispositivo legítimo de autenticação criptográfica; assim, frustrando tentativas comuns de clonagem. Fornecer um método periódico de renovação de desafio-resposta aumentaria a segurança removendo qualquer comprometimento existente, pois cada atualização incremental de aplicativo poderia substituir a lista de pares de desafio-resposta. A Figura 3-1 ilustra a operação desse modelo de segurança.

Figura 3-1. Anticlonagem / Antipirataria



As empresas também podem querer identificar placas autênticas antes de fornecer suporte técnico. Uma interface poderia ser implementada que permitiria ao usuário inserir qualquer sequência de texto que, por sua vez, seria alimentada ao dispositivo ATSHA204 na placa de desenvolvimento e a resposta exibida ao usuário. O operador de suporte técnico pode verificar o sistema fornecendo ao usuário uma string personalizada e solicitando a resposta gerada. O operador do help desk seria então capaz de verificar a autenticidade da placa de desenvolvimento antes de prestar serviço ao cliente.

4. Troca de chave de sessão

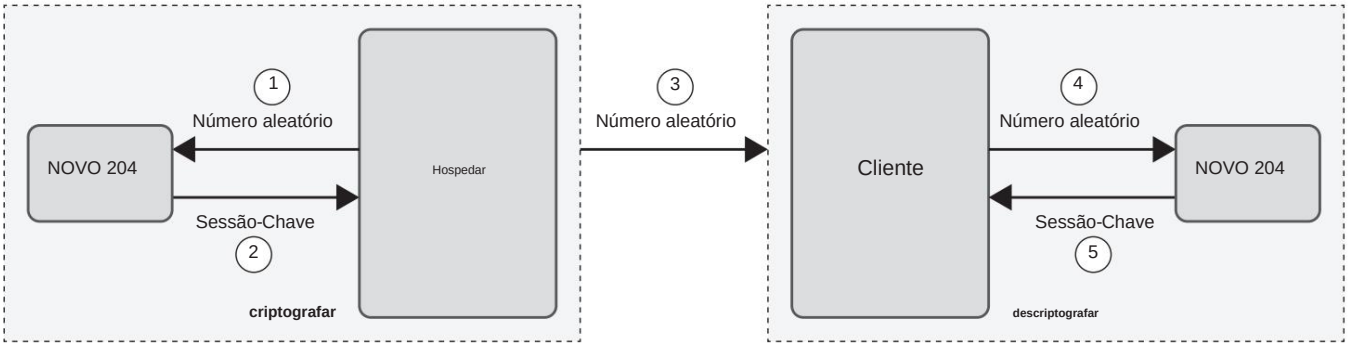
A ATSHA204 CryptoAuthentication também pode ser usada para troca segura de chaves. Nesse esquema, o ATSHA204 é usado em conjunto com um algoritmo de criptografia simétrica, como AES ou DES. ATSHA204 pode facilitar isso usando a resposta única produzida pelo dispositivo como uma chave para o algoritmo de criptografia simétrica.

Para garantir a exclusividade da chave de criptografia, é necessário um número aleatório no processo de geração. Esse número aleatório é usado para gerar uma chave de sessão exclusiva. O número aleatório pode ser uma constante, algo relacionado ao sistema atual ou um número aleatório obtido do ATSHA204.

A troca de chaves é feita enviando um desafio aleatório para o Host ATSHA204, que gera uma resposta que é usada como chave de sessão para criptografar a mensagem. A mensagem e o desafio aleatório são então enviados ao cliente ATSHA204. No lado do cliente, o desafio aleatório é alimentado no ATSHA204 para gerar a resposta que é usada como chave para descriptografar a mensagem. Deve-se observar que a chave raiz é a mesma no host e no cliente.

A Figura 4-1 ilustra como criptografar e descriptografar vários arquivos usando a chave gerada pelo ATSHA204.

Figura 4-1. Troca de chave de sessão usando ATSHA204



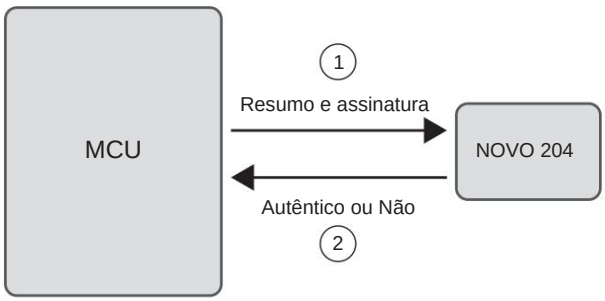
5. Inicialização segura

Os sistemas modernos geralmente são construídos usando um microprocessador padrão com o programa operacional armazenado na memória flash. Essa arquitetura pode permitir que o fabricante aproveite rapidamente os avanços no desempenho do processador e no custo da memória, ao mesmo tempo em que oferece um rápido tempo de lançamento no mercado. Se o programa operacional estiver armazenado em um dispositivo Flash externo, é muito difícil impedir que um adversário obtenha seu conteúdo e o modifique para executar um programa fraudulento. Ao usar o ATSHA204 no sistema, o fabricante pode garantir que apenas o programa autêntico possa ser executado no sistema.

Para implementar a inicialização segura, um código ou assinatura de validação é armazenado em flash junto com o programa operacional. Como parte da execução do programa de inicialização na inicialização do sistema, o dispositivo de segurança verifica a assinatura para garantir que o programa seja autêntico. Se a verificação for bem-sucedida, o programa operacional é executado e o sistema opera normalmente. Qualquer modificação do programa operacional, mesmo um único bit, exigirá uma nova assinatura de validação.

O esquema de inicialização segura é ilustrado na Figura 5-1.

Figura 5-1. Modo de segurança



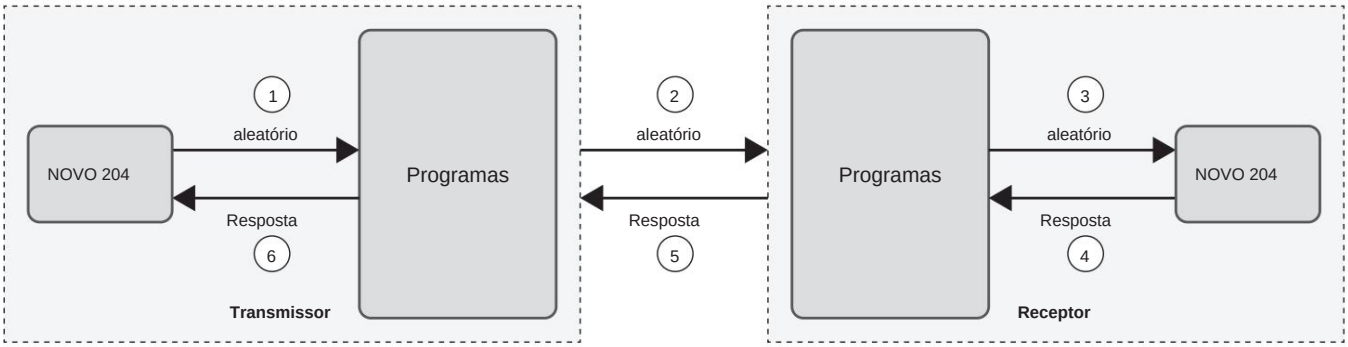
Além disso, o fabricante também é capaz de garantir que apenas um sistema autêntico possa executar o programa por meio da autenticação mútua. A autenticação mútua é suportada pelo ATSHA204 usando a operação de cópia CheckMac.

6. Segurança de rede

Os dispositivos de transmissão sem fio precisam verificar cada nó antes de permitir o acesso à rede. ATSHA204 CryptoAuthentication é uma ótima opção para oferecer um método de verificação de baixo custo. Ao instalar dispositivos ATSHA204 nos nós de rádio (Client), o nó transmissor (Host) pode verificar se está se comunicando com nós de rede válidos antes de transmitir comandos ou informações importantes. Segurança adicional pode ser alcançada adicionando outro dispositivo ATSHA204 no Host para que os segredos do cliente não precisem ser mantidos no código do microprocessador onde desenvolvedores e subcontratados podem ter acesso a eles. Ao usar ATSHA204 adicional no nó de transmissão, ambos ATSHA204 devem concordar com o mesmo valor de chaves.

A Figura 6-1 ilustra uma configuração que utiliza dois dispositivos ATSHA204 em uma rede de rádio.

Figura 6-1. Autenticação de nó sem fio

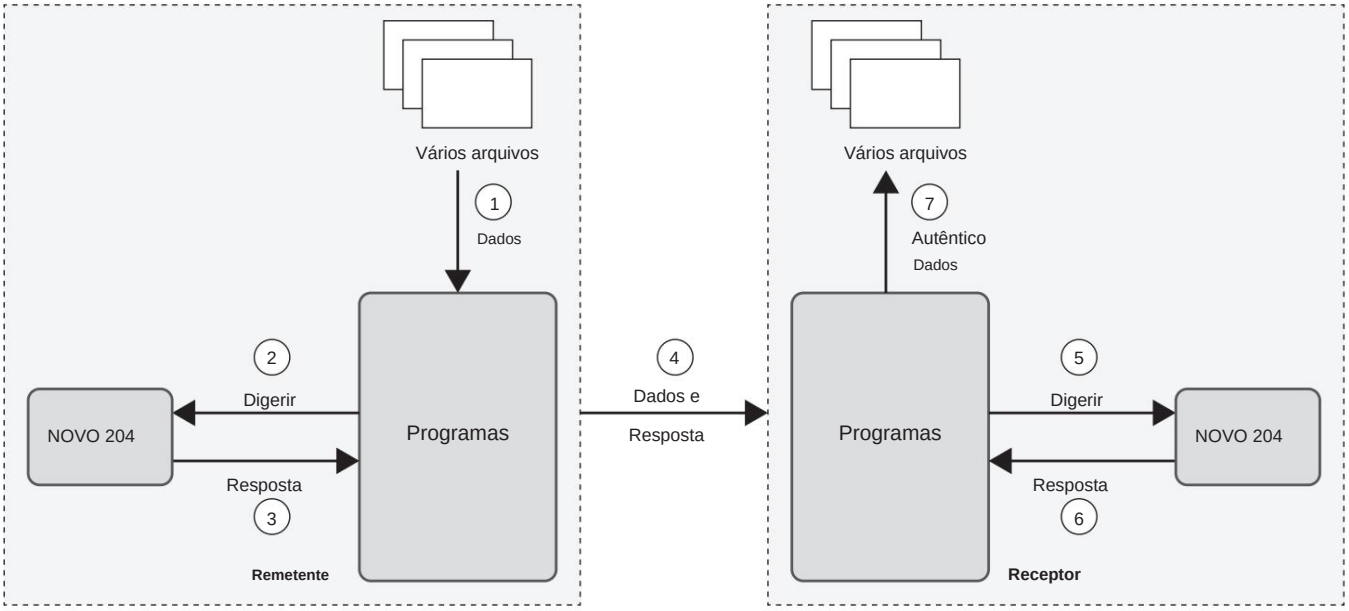


Um nível adicional de segurança pode ser adicionado aos dados que estão sendo transferidos, ou seja, criptografar os dados ou apenas verificar a integridade dos dados. O processo de criptografia pode ser aplicado exatamente como o esquema de criptografia de dados mostrado acima.

A integridade dos dados que estão sendo trocados também pode ser verificada. Antes de enviar os dados, o remetente calcula o resumo de dados usando o algoritmo SHA-256. Em seguida, o ATSHA204 calcula a resposta usando o resumo de dados como desafio.
A resposta calculada é enviada junto com os dados para o lado do receptor. Ao receber, o receptor calcula o resumo de dados e a resposta compara a resposta recebida com a resposta calculada. Se as respostas corresponderem, significa que os dados não foram adulterados por nenhum invasor.

A Figura 6-2 ilustra uma configuração que utiliza dois dispositivos ATSHA204 em uma rede de rádio.

Figura 6-2. Verificação da integridade dos dados



Esta configuração pode ser aplicada a estes aplicativos:

- ÿ Autenticação de nó sem fio
- ÿ Autenticação de dados sobre linhas de energia

7. Chaves rolantes

Em alguns aplicativos, usar a mesma chave repetidamente pode ser um risco à segurança. Por exemplo, abridores de portas de garagem. O ATSHA204 fornece um recurso para chaves rolantes. Normalmente, após um certo número de usos (talvez apenas um), o valor da chave atual é substituído pelo resumo SHA-256 de seu valor atual combinado com algum deslocamento. O deslocamento pode ser uma constante, algo relacionado ao sistema atual ou um número aleatório.

Um uso para esse recurso é remover permanentemente a chave original do dispositivo; substituindo-o por uma chave que só é útil em um determinado ambiente. Depois que a chave é rolada, não há como recuperar o valor antigo, o que melhora a segurança do sistema.

Existem dois tipos de processo de Rolling Key:

- **Rolled Keys** — Usa o valor da chave atual para gerar uma nova chave, a chave gerada é chamada Rolled Keys.
- **Chaves criadas** — Usa o valor de uma chave pai para gerar uma nova chave, a chave gerada é chamada de Chaves criadas.

Esta operação só pode ser executada em um slot que permita o comando DeriveKey. A configuração adequada deve ser definida no slot escolhido. Para executar a operação, o Nonce deve ser executado primeiro para preencher o valor TempKey e, em seguida, o comando DeriveKey é executado visando o slot escolhido. Após a execução do comando, o valor do slot de destino será atualizado com o resumo gerado pelo comando DeriveKey.

8. Resumo

A funcionalidade multifuncional do dispositivo ATSHA204 CryptoAuthentication os torna uma ferramenta excepcional para habilitar a segurança de hardware. Praticamente qualquer aplicativo que exija autenticação ou identificação individual de nós pode usar o ATSHA204 como parte de sua arquitetura de solução de segurança. Se seus requisitos de segurança forem diferentes dos listados neste documento, ou se você não tiver certeza de que os dispositivos ATSHA204 CryptoAuthentication são adequados para sua aplicação específica, entre em contato com o representante local da Atmel. É provável que a Atmel tenha um produto que atenda às suas necessidades.

Apêndice A. Documentos de suporte

ÿ Usos do produto CryptoAuthentication para Atmel AT88SA10HS e Atmel AT88SA102S. Por favor visite, http://www.atmel.com/Images/doc8663.pdf.

Apêndice B. Histórico de revisões

Doc. Rev.	Data	Comentários
8794A	12/2012	Liberação inicial do documento.

Enabling Unlimited Possibilities®

Atmel Corporation
Unidade de Tecnologia 1600
São José, CA 95110
cervo
Tel: (+1) (408) 441-0311
Fax: (+1) (408) 487-2600
www.atmel.com

Atmel Asia Limited
Unidade 01-5 e 16, 19F
Torre BEA, Millennium City 5
418 Kwun Tong Roa
Kwun Tong, Kowloon
HONG KONG
Tel: (+852) 2245-6100
Fax: (+852) 2722-1369

Atmel Munich GmbH
campus de negócios
Estacionamento 4 D-85748 Garching b. Munique
ALEMANHA
Tel: (+49) 89-31970-0
Fax: (+49) 89-3194621

Atmel Japão GK
16F Shin-Osaki Kangyo Bldg 1-6-4
Osaki, Shinagawa-ku Tóquio
141-0032
JAPÃO
Tel: (+81) (3) 6417-0300
Fax: (+81) (3) 6417-0370