Trabalhando com Assinaturas Digitais

Aplicação da tecnologia

As assinaturas digitais são recomendadas em uma variedade de situações onde a autenticidade, integridade e não repúdio são importantes. Algumas situações em que as assinaturas digitais são comumente utilizadas são:

1. **Documentos Legais e Contratos**: Em transações comerciais e legais, as assinaturas digitais podem ser usadas para autenticar contratos, acordos e outros documentos importantes. Isso garante que as partes envolvidas não possam negar posteriormente sua participação no acordo.
2. **Transações Financeiras**: Em sistemas de pagamento online, como transações bancárias eletrônicas, as assinaturas digitais são usadas para garantir a autenticidade das transações e a integridade dos dados financeiros transmitidos.
3. **E-mails Seguros**: As assinaturas digitais podem ser aplicadas em e-mails para garantir que o remetente seja autenticado e que o conteúdo da mensagem não tenha sido alterado durante a transmissão.
4. **Software e Atualizações**: Assinaturas digitais são usadas para verificar a autenticidade e a integridade de software e atualizações distribuídas pela Internet. Isso ajuda a prevenir a distribuição de software malicioso ou modificado.
5. **Certificação Digital**: Em muitas jurisdições, as assinaturas digitais são utilizadas para emitir certificados digitais que autenticam a identidade de indivíduos, organizações e servidores online.

Possibilidade de aplicação em softwares de gestão

A aplicação do conceito de Assinatura Digital a um software de gestão, pode ocorrer onde as assinaturas digitais sejam necessárias em várias situações como:

- **Documentos e Contratos**: Os softwares de gestão podem incluir recursos para assinar digitalmente documentos e contratos, proporcionando autenticidade e não repúdio.
- **Aprovações e Autorizações**: Em processos de aprovação internos, como pedidos de compra, relatórios de despesas ou folhas de pagamento, as assinaturas digitais podem ser usadas para formalizar e autenticar as aprovações.
- **Transações Financeiras**: Em sistemas de gestão financeira, as assinaturas digitais podem ser aplicadas em transações, garantindo a autenticidade e a integridade das operações realizadas.
- **Auditoria e Conformidade**: Os softwares de gestão podem utilizar assinaturas digitais para registrar e autenticar auditorias, registros de alterações e outras atividades relacionadas à conformidade regulatória.

Visão de Negócio

Você deve construir um software de gestão que permita aos funcionários de uma empresa submeter relatórios de despesas de viagens para aprovação e reembolso. Neste cenário, a técnica de assinatura digital pode ser aplicada da seguinte forma:

1. **Submissão do Relatório de Despesas**: Um funcionário utiliza o software de gestão para submeter um relatório de despesas contendo detalhes sobre suas despesas comerciais, como recibos digitalizados, datas, valores e descrições das despesas. O gestor do funcionário deverá receber uma mensagem de aviso sobre um novo relatório submetido.
2. **Aprovação pelo Gestor**: O relatório de despesas é encaminhado para o gestor responsável pela aprovação. Antes de aprovar, o gestor revisa as despesas relatadas e verifica sua legitimidade.
3. **Assinatura Digital do Gestor**: Após revisão e aprovação, o gestor utiliza sua chave privada para assinar digitalmente o relatório de despesas. Essa assinatura digital atesta a autenticidade da aprovação e garante a integridade dos dados no relatório.
4. **Registro no Sistema**: O software de gestão registra a assinatura digital do gestor juntamente com o relatório de despesas aprovado. Isso cria um registro imutável da aprovação, incluindo a identidade do gestor e o momento em que a aprovação ocorreu. O funcionário deve receber uma mensagem de aviso indicando que seu relatório foi aprovado e assinado.
5. **Processamento do Reembolso**: Com o relatório de despesas devidamente aprovado e assinado digitalmente, o sistema pode iniciar o processo de reembolso ao funcionário. A assinatura digital fornece garantias adicionais de que o relatório foi aprovado pelo gestor autorizado.
6. **Auditoria**: Um diretor poderá acessar o relatório assinado por um gestor e verificar a validade da assinatura digital.

Nesta situação, a técnica de assinatura digital é aplicada durante o processo de aprovação de despesas, proporcionando segurança e confiabilidade ao processo. Ela ajuda a garantir que apenas despesas aprovadas por gestores autorizados sejam reembolsadas, evitando fraudes e manipulações. Além disso, as assinaturas digitais criam um registro auditável das aprovações, que pode ser utilizado para fins de conformidade e prestação de contas.

Pipeline de desenvolvimento

Sugiro que você proceda da seguinte maneira:

1. **Configuração do Ambiente de Desenvolvimento**: Certifique-se de ter um ambiente de desenvolvimento configurado com PHP, MySQL e um servidor web (como Apache). Você também precisará de um editor de texto ou IDE para escrever seu código. Sugiro usar XAMPP e VS Code.
2. **Estrutura do Banco de Dados**: Crie uma estrutura de banco de dados MySQL para armazenar:
    a. Colaboradores, diferenciando-os entre funcionários, gerentes e diretores.
    b. Relatórios de despesas
    c. Assinaturas digitais.
3. **Desenvolvimento do Frontend (HTML/CSS + JavaScript)**: Crie interfaces de usuário para permitir que os funcionários façam login no sistema, submetam relatórios de despesas e que os gestores os aprovem. Utilize HTML, CSS e JavaScript para construir as páginas necessárias, incluindo formulários para submissão e visualização de relatórios.
4. **Implementação do Backend (PHP ou outra tencologia)**: Desenvolva o backend para lidar com a lógica de negócios, processamento de formulários, interações com o banco de dados e geração/verificação de assinaturas digitais. Por exemplo:
    a. Criar scripts para receber dados dos formulários, validar entradas e inserir/alterar registros no banco de dados.
    b. Implementar funcionalidades para gerar e verificar assinaturas digitais utilizando bibliotecas adequadas de criptografia, como OpenSSL.
    c. Desenvolver lógica para enviar notificações por e-mail aos funcionários e gestores quando houver a submissão ou aprovação de um relatório de despesas.
5. **Integração com Bibliotecas de Criptografia**: Utilize bibliotecas de linguagem server-side e JavaScript para lidar com operações de criptografia e geração de chaves assimétricas. Por exemplo, você pode usar a extensão OpenSSL em PHP e bibliotecas JavaScript como CryptoJS ou libsodium.js.
6. **Testes e Depuração**: Realize testes para garantir que todas as funcionalidades estejam funcionando conforme o esperado. Teste diferentes cenários, como submissão de relatórios, aprovação/rejeição pelos gestores e verificação de assinaturas digitais.
7. **Implementação de Segurança**: Certifique-se de implementar medidas de segurança adequadas para proteger os dados sensíveis, como proteção contra ataques comuns, como injeção de SQL e XSS.

Uma sugestão de implementação

Abaixo segue uma sugestão das páginas necessárias para criar a aplicação com base nos requisitos acima:

1. Página de Login:

   login.html: Página de login para autenticar os usuários.

2. Página Principal (Após Login):

   dashboard.php: Página principal após o login, mostrando opções para CRUD de funcionários e cadastro de relatórios de despesas.

3. CRUD de Funcionários:

   listar_funcionarios.php: Página para listar todos os funcionários.

   cadastrar_funcionario.php: Página para cadastrar novos funcionários, incluindo a indicação de Gerente ou Diretor.

4. Cadastro de Relatório de Despesa:

   cadastrar_despesa.php: Página para o funcionário cadastrar um novo relatório de despesa, com formulário para upload do arquivo PDF contendo os recibos.

5. Notificação por E-mail:

   enviar_email.php: Script PHP para enviar e-mails de notificação ao gerente quando um novo relatório de despesa for cadastrado.

6. Validação de Relatório pelo Gerente:

   listar_despesas_pendentes.php: Página para o gerente listar os relatórios de despesa pendentes de validação.

   validar_despesa.php: Página para o gerente visualizar e validar os relatórios de despesa, com opção para assinar digitalmente.

7. Assinatura Digital:

   assinar_despesa.php: Página para o gerente assinar digitalmente o relatório de despesa validado.

8. Notificação ao Funcionário:

   notificar_funcionario.php: Script PHP para enviar e-mails de notificação ao funcionário quando seu relatório de despesa for validado e assinado pelo gerente.

9. Verificação de Assinaturas pelo Diretor:

   listar_despesas_assinadas.php: Página para o diretor listar os relatórios de despesa que foram assinados.

   verificar_assinatura.php: Página para o diretor verificar a veracidade das assinaturas digitais nos relatórios de despesa.

Uma sugestão de estrutura do banco de dados

Para este software que envolve o CRUD de funcionários, cadastro de relatórios de despesas e assinaturas digitais, sugiro a seguinte estrutura de banco de dados.

Tabelas:

1. Funcionários:

- id (chave primária)
- nome
- email
- cargo (Funcionário, Gerente, Diretor, etc.)
- senha (criptografada)

2. Relatórios de Despesas:

- id (chave primária)
- funcionario_id (chave estrangeira referenciando o funcionário que cadastrou o relatório)
- data
- descricao
- valor
- arquivo_pdf (caminho para o arquivo PDF com os recibos)
- status (pendente/aprovado/rejeitado)

3. Assinaturas Digitais:

- id (chave primária)
- relatorio_id (chave estrangeira referenciando o relatório de despesa)
- gerente_id (chave estrangeira referenciando o gerente que assinou o relatório)
- data
- assinatura (armazenar a assinatura digital)

Relacionamentos:

- Um funcionário pode ter vários relatórios de despesas, portanto, há uma relação de um para muitos entre a tabela Funcionários e Relatórios de Despesas.
- Cada relatório de despesa pode ter uma ou mais assinaturas digitais de gerentes, o que implica em uma relação de um para muitos entre a tabela Relatórios de Despesas e Assinaturas Digitais.
- A tabela Assinaturas Digitais referencia tanto o relatório de despesa quanto o gerente que assinou o relatório.

Bibliotecas e Tecnologias

Para criar as páginas assinar_despesa.php e verificar_assinatura.php, você precisará de tecnologias específicas para lidar com a geração e verificação de assinaturas digitais.

Sugiro o uso das seguintes bibliotecas:

- OpenSSL: Uma biblioteca amplamente utilizada para criptografia assimétrica em PHP.
- PHPMailer: Para enviar e-mails de forma fácil e segura em PHP.
- FPDF: Uma biblioteca PHP para criação de arquivos PDF.
- FPDI: Uma extensão do FPDF que permite importar páginas de outros documentos PDF.