

CENTRO UNIVERSITÁRIO FUNDAÇÃO SANTO ANDRÉ
ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

ANTHONY DIONISIO DOS SANTOS
RA:746761

CERTIFICAÇÃO DIGITAL

SANTO ANDRÉ – SP

2023

ANTHONY DIONISIO DOS SANTOS

RA:746761

CERTIFICAÇÃO DIGITAL

Resumo solicitado pelo professor, como complemento da nota de atividade da disciplina de Segurança da Informação.

Orientador: Felipe José dos Santos Bastos

SANTO ANDRÉ – SP

2023

Sumário

1. Introdução.	4
2. o que é a certificação digital	4
3. Benefícios da certificação digital.....	5
4. Tipos de certificado digital.....	5
5. Assinatura Digital	6
6. Conclusão	6

1. INTRODUÇÃO.

Antes da chegada da certificação digital, o mundo das transações e comunicações eletrônicas era marcado por uma grande insegurança. A autenticidade e a integridade das informações eram facilmente comprometidas, o que gerava um grande risco para a realização de transações bancárias, assinaturas de documentos e outros tipos de operações eletrônicas. Com o avanço da tecnologia, a necessidade de garantir a segurança das informações em ambiente eletrônico se tornou cada vez mais premente. Nesse contexto, a certificação digital surgiu como uma solução inovadora e eficiente para proteger a privacidade e a confidencialidade das informações transmitidas eletronicamente. A partir de então, essa tecnologia passou a ser uma ferramenta essencial para garantir a segurança das transações eletrônicas em todo o mundo.

2. O QUE É A CERTIFICAÇÃO DIGITAL

A certificação digital é uma tecnologia que permite a verificação da autenticidade de um documento eletrônico. Isso é feito através da utilização de um certificado digital, que é emitido por uma autoridade certificadora (AC) confiável. O certificado digital é um arquivo eletrônico que contém informações sobre a identidade do titular, a chave pública e a assinatura digital da AC.

A assinatura digital é um processo que garante a integridade e a autenticidade do documento eletrônico. Ela é gerada a partir de uma chave privada do titular do certificado digital, que é única e não pode ser reproduzida. Quando o documento é assinado digitalmente, a assinatura digital é verificada pelo receptor utilizando a chave pública contida no certificado digital do emissor.

A certificação digital tem uma ampla aplicação, desde transações bancárias, até assinatura de documentos digitais, como contratos, declarações e outros documentos que requerem autenticação. A certificação digital também é utilizada para garantir a privacidade das informações, através da criptografia dos dados transmitidos.

A importância da certificação digital é evidente em um mundo cada vez mais digital. Com a crescente utilização de dispositivos eletrônicos para transações e comunicações, a certificação digital se tornou fundamental para garantir a segurança dessas transações. Sem a certificação digital, a autenticidade e a integridade das informações em ambiente eletrônico ficam comprometidas.

3. BENEFÍCIOS DA CERTIFICAÇÃO DIGITAL

A certificação digital traz inúmeros benefícios para o mundo das transações e comunicações eletrônicas. Um dos principais é a segurança, uma vez que essa tecnologia garante a autenticidade e a integridade das informações transmitidas eletronicamente. Além disso, a certificação digital também é capaz de proteger a privacidade e a confidencialidade das informações, por meio da criptografia dos dados transmitidos. Outro benefício importante da certificação digital é a praticidade, pois ela permite a realização de transações e assinaturas de documentos de forma remota, sem a necessidade de deslocamentos físicos. Isso reduz custos e agiliza processos, tornando a vida dos usuários muito mais fácil. Por fim, a certificação digital também traz benefícios econômicos, pois reduz a burocracia e a papelada envolvida nas transações eletrônicas, o que pode gerar economias significativas para empresas e governos.

4. TIPOS DE CERTIFICADO DIGITAL

Existem diversos tipos de certificados digitais, cada um com suas particularidades e funcionalidades específicas. Uns dos mais comuns são os certificados digitais dos tipos A e S. Estes tipos de certificados digitais possuem diferentes subclasses que atendem às necessidades específicas dos usuários. No caso do certificado digital A, existem as subclasses A1, A2, A3 e A4 e no caso do certificado digital S existem as subclasses S1, S2, S3 e S4. Os certificados digitais A1 e S1 são válidos apenas para uma sessão e é gerado automaticamente pelo computador ou dispositivo móvel do usuário, armazenado em um dispositivo externo. Já o certificado digital A2 e S2 são armazenados em um token USB ou em um cartão inteligente e possuem validade de até dois anos. Os certificados digitais A3 e S3, por sua vez, são armazenados em um cartão inteligente e possuem validade de até três anos. Os certificados digitais A4 e S4 são armazenados em um dispositivo móvel, como um smartphone, e possuem validade de até três anos. Os certificados mais comuns são os do tipo A1 e A3.

5. ASSINATURA DIGITAL

A assinatura digital é uma das principais funcionalidades dos certificados digitais, permitindo que o usuário assine eletronicamente documentos, contratos, e-mails, entre outros. A assinatura digital é uma forma de comprovar a autenticidade e integridade do documento assinado, bem como a identidade do signatário. Para assinar um documento digitalmente, o usuário deve ter um certificado digital válido e utilizar um software específico para a assinatura digital. Ao assinar um documento digitalmente, o certificado digital do signatário é utilizado para criar um conjunto de dados que é anexado ao documento, comprovando a autenticidade e integridade do documento assinado. A assinatura digital é uma tecnologia essencial para a segurança das transações eletrônicas, permitindo que documentos importantes sejam assinados de forma segura e eficiente, sem a necessidade de impressão ou envio físico dos documentos.

6. CONCLUSÃO

A certificação digital é uma tecnologia fundamental para garantir a segurança e autenticidade das transações eletrônicas. Através dos certificados digitais, é possível comprovar a identidade dos usuários, assinar digitalmente documentos, contratos, e-mails, entre outros, além de garantir a integridade e autenticidade dos dados transmitidos. Com o aumento da digitalização dos processos e a crescente utilização de meios eletrônicos para as transações comerciais e financeiras, a certificação digital torna-se cada vez mais importante e necessária. É importante que as empresas e usuários estejam cientes da importância da segurança nas transações eletrônicas, e que utilizem certificados digitais devidamente emitidos por autoridades certificadoras confiáveis, a fim de garantir a segurança e confiabilidade das transações eletrônicas realizadas.