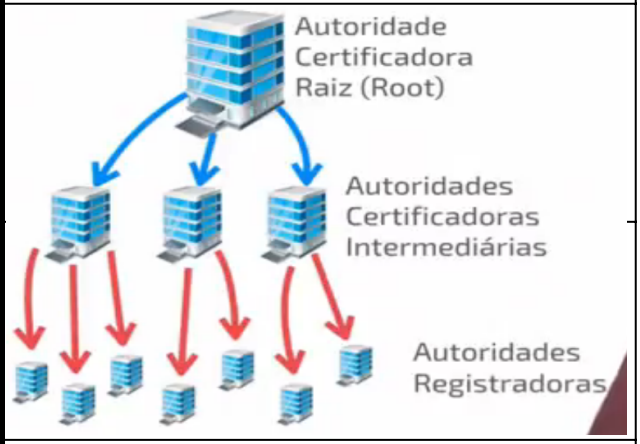
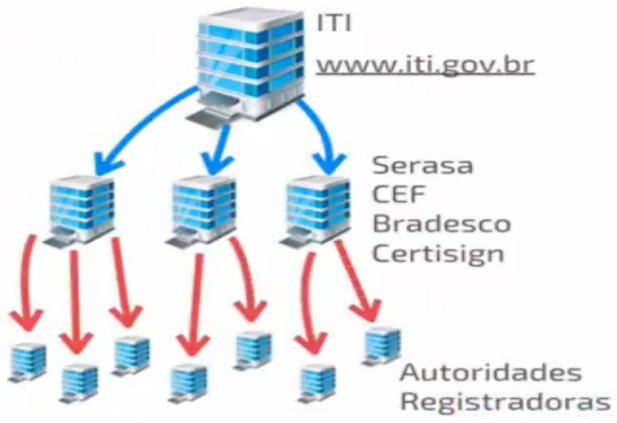
CERTIFICAÇÃO DIGITAL	CERTIFICAÇÃO DIGITAL
O que é uma **Certificação Digital**?	**Certificação Digital:** É um documento - geralmente digital - que garante que uma Chave Pública **é legítima**, tornando essa chave um objeto institucionalizado. Esse processo é feito por através de órgãos certificadores que validam a autenticidade e efetividade de uma determinada Chave Pública de um determinado usuário. Todo certificado tem data de validade e precisam ser auditorados dentro do prazo de validade, para que seja feita a reciclagem da Certificação Digital.
Por que existe a **necessidade de certificação** das Chaves Públicas?	Como havemos de lembrar as Chaves Públicas são criadas a partir de uma Chave Privada dentro do computador de um usuário, ou seja, elas não são criadas pelos desenvolvedores dos sistemas num local segregado somente para isso, mas **são criadas no próprio algoritmo do usuário. Daí surgiram as grandes dúvidas, devo confiar a qualquer usuário a garantia de que sua chave pública é legítima? E se eu me deparar com um usuário mau intencionado?** Daí surgiu a necessidade de procurar por órgãos certificadores que garantem que as Chaves Públicas criadas dentro dos computadores dos usuários
Que **alertas** podem ser gerados em um site ou aplicativo que tiver **problemas com seu Certificado**?	**- Site sem Certificação** (Alguns protocolos da internet, como o HTTPS, avisam que o site ou aplicação é inseguro por não ter certificação); **- Certificados Expirados** (Fora da Data de Validade); **- Certificado Revogado** (quando o dono revogou o certificado, mas ainda está sendo usado - isso pode ser um sinal de alerta, afinal o site pode estar sendo usado por outra pessoa); **- Certificado de Outro Titular** (O certificado aponta para outro site ou programa, pode ser uma falsidade ideológica); **- Certificado de Órgão não-confiável;**
O que é uma **PKI**?	**PKI:** Ou **Public Key Infrastructure** no Brasil é conhecida como **ICP (Instrutura de Chave Pública)**, é uma **rede de órgãos públicos e privados que trabalham em conjunto para garantir que o uso e geração de Chaves Públicas seja definido segundo normas regularizadoras, seguindo boas práticas de implementação e uso de diretrizes legais e infraestruturais das redes.** No Brasil temos a ICP-Brasil, uma infraestrutura que conta com a colaboração de órgãos públicos como a ITI e privados para monitorar o uso de Chaves Públicas e Certificações de usuários.
Quais são os **componentes** de uma PKI?	Toda PKI tem o seguintes componentes: **- AC RAIZ:** Autoridade Certificadora Raiz ou (Root), geralmente Federal, e responsável por todas as outras autoridades certificadoras do país; **- AC Intermediárias:** Órgãos Privados que trabalham sobre a supervisão da AC Root, responsáveis por certificar usuários de Chaves Públicas; **- AR:** Ou Autoridades Registradoras, são empresas que prestam serviço para as AC Intermediárias fazendo o contato direto como cliente;
Ilustre como funciona a Rede Infraestrutural de uma PKI	
- reservado para a questão acima -	
Como funciona uma **AC Root**?	**AC Root:** Ou **Autoridade Certificadora Raiz**, é onde toda a estrutura de uma PKI está organizada, a AC Root geralmente é um órgão Federal - como o ITI aqui no Brasil - que é **responsável por manter a ordem e usabilidade das Chaves Públicas em todo o país.** Por isso ela monitora as Autoridades Certificadoras Intermediárias, assinando os seus certificados, ela não assina os certificados dos usuários final, essa assinatura fica a cargo das AC Intermediárias. Por ser a autoridade máxima, a AC Root assina o seu próprio certificado de qualidade, além disso, ela que é responsável por emitir a LCR ou Lista de Certificados Revogados.
Como funciona uma **AC Intermediária**?	**AC Intermediária:** ou **Autoridade Certificadora Intemediária**, são os órgãos privados que estão debaixo da autoridade da AC Root e são **responsáveis por assinar os certificados dos usuários finais**, como: Pessoas Físicas, Jurídicas ou Sites. É importante que o usuário se atente a procurar uma AC Intermediária que foi Certificada pela AC Root para evitar problemas de certificação ao utilizar o seus sistema.
Como funciona uma **AR**?	**AR:** ou **Autoridade de Registro**, são orgãos privados que NÃO CERTIFICAM, NEM EMITEM, NEM REVOGAM qualquer certificado, em vez disso, o trabalho das ARs é **fazer o meio campo entre o cliente que deseja a certificação e as AC Intermediárias.** O cliente deve procurar a AR para ficar a par de todas as requisições necessárias para que ele possa conseguir sua certificação. Além disso, as ARs são usadas pelas AC Intermediárias para informar aos usuários revogações de contratos, expirações e etc.

CERTIFICAÇÃO DIGITAL	CERTIFICAÇÃO DIGITAL
Como a **ICP-Brasil está estruturada**?	A ICP-Brasil está estruturada com as seguintes entidades: - **AC Root:** Temos a ITI (www.iti.gov.br), ela é a autoridade máxima no assunto de Chaves Públicas em todo o Brasil; - **AC Intermediárias:** Podemos alistar algumas como Serasa, CEF, Bradesco, Certisign, entre outras; - **Autoridades de Registradoras**: temos várias, basta entrar em contato com as AC intermediarias e pedir o contato delas e elas apresentarão uma lista de autoridades que podemos procurar para nos ajudar numa certificação;
Ilustre a estrutura de organização do ICP-Brasil	
- reservado para a questão acima -	
Quais são alguns **tipos de certificados** oferecidos pela ICP-Brasil?	Alguns certificados oferecidos pela ICP-Brasil são: - **Tipo A (Autenticidade):** Certificados para Assinatura Digital; - **Tipo S (Sigilo):** Ceritificados para Criptografia, para pessoas que desejam implementar um sistema de criptografia; - **Tipo T (Time Stamp):** Certificados para garantir a data e hora que uma determinada Assinatura Digital foi assinada, para ser usada como compravação de uso da chave; Esses tipos de certificado podem ser mesclados, como geralmente acontece, como os certificados: **A1/S1** (válido por 1 ano) **A3/S3** (válido por 3 anos) **A4/S4** (válido por 6 anos). Os certificados vão variar para tipos de usuário, tempos de expiração, tipos de aplicação, tamanhos de chaves e etc.
- reservado para a questão acima -	