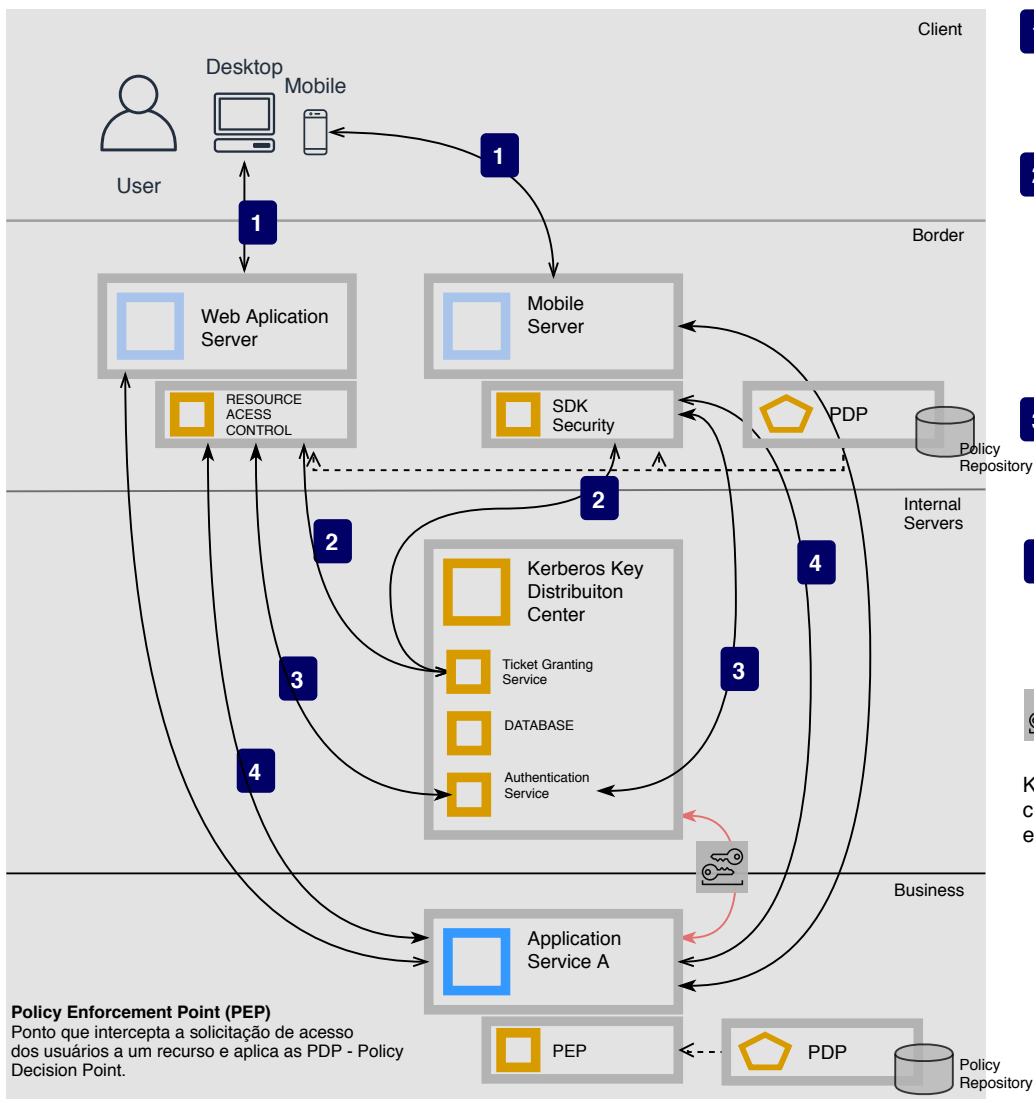



AUTHENTICATION KERBEROS PROTOCOL REFERENCE ARCHITURE



- 1** usuário requisita acesso ao recurso Application Service A
serviço de segurança RCA/SDK (PEP) verifica requisitos de acesso e autorização
se usuário não autenticado realiza identificação/autenticação
 - 2 User Authentication (Get a TGT)**
O RAC/SDK (has Client Kerberos - CK function) que realize a identificação/autenticação do usuário
o CK solicita ao KDC/Authentication Service que gere o TGT (ticket de concessão de "acesso") para o usuário.
o Authentication Service gera o TGT e criptografa com base na senha do usuário e devolve o TGT ao RAC/SDK.

o RAC/SDK solicita ao usuário a senha de forma a verificar se o TGT é descriptografado:
se descriptografado com sucesso: a senha está correta <- o RAC/SDK mantém TGT descriptografado pois é a prova a identidade do usuário
 - 3 User Authorization (Get a Service Ticket)**
o RCA/SDK apresenta o TGT ao TGS (Ticket Granting Service) e requisita o Ticket de concessão de acesso para o Serviço (Service Ticket).
o KDC/TGS gera o Service Ticket e devolve ao RAC/SDK.
 - 4 Service Request (start Service Session)**
o RAC/SDK apresenta o Service Ticket ao Application Service A.
o Security Service PEP verifica o Service Ticket e autoriza o RCA/SDK garantindo o acesso ao recurso.
o Application Service A estabelece a sessão do usuário.
-  É requisito o compartilhamento de Chaves Criptográficas de Longo prazo entre o KDC e o Application Service.
criptografar do Ticket de Serviço.

Kerberos é um protocolo de autenticação de rede. Ele foi projetado para fornecer autenticação forte para aplicativos cliente / servidor usando criptografia de chave secreta. A arquitetura Kerberos é projetada em torno da troca de mensagens entre três tipos de entidades:

- Os clientes que usam serviços kerberos.
- Os servidores que fornecem serviços (os clientes e os servidores são coletivamente referidos como principais).
- Os servidores que gerenciam o próprio protocolo Kerberos. Esses servidores geralmente são chamados de KDCs

(Key Distribution Centers) e incluem vários serviços modulares.

KERBEROS DATABASE

O banco de dados - BD Kerberos contém todos os usuários Kerberos de um domínio, suas senhas e outras informações administrativas sobre cada usuário.

- kdb5_util Program: permite manipular o BD Kerberos como um todo
- kadmin Program: permite fazer alterações nas entradas no banco de dados.
- kpasswd program: permite a alteração das senhas pelos usuários.

A vantagem do sistema de autenticação Kerberos é que cada serviço recebe apenas o ticket para esse serviço. Um cliente não entrega sua senha e, portanto, o serviço não conhece a senha do cliente o que elimina o risco do serviço usá-la para se passar por usuário.

COMO O KERBEROS FUNCIONA

O sistema de autenticação Kerberos é construído sobre tickets (também chamados de credenciais). A ideia principal por trás do Kerberos é que um cliente não fornece a senha da conta para cada serviço com o qual deseja interagir. Em vez disso, um cliente envia uma solicitação de emissão de Ticket de concessão de acesso para o Serviço ao Centro de Distribuição de Chaves (KDC).

Ticket de concessão de acesso ao Serviço (Service Ticket): é o elemento que permite o acesso ao Serviço sendo válido apenas para o Serviço requisitado.

Um Ticket de Serviço é criptografado com uma chave de serviço, que é uma chave de longo prazo compartilhada entre o KDC (Key Distribution Center) e o serviço de destino (Application Service A).

Somente o KDC e o serviço de destino podem ler tickets, permitindo acesso seguro às credenciais do usuário, à chave da sessão e outras informações.

REFERÊNCIAS

RFC 4120 - The Kerberos Network Authentication Service (V5) disponível em <https://tools.ietf.org/html/rfc4120>
Kerberos Authentication disponível em <https://docs.bmc.com/docs/sso81/kerberos-authentication-481024664.html>
MIT Kerberos Documentation disponível em <https://web.mit.edu/kerberos/krb5-1.12/doc/admin/database.html>

RAC - Resource Access Control <- implementa o serviço de controle de acesso ao recurso
Os serviços de controle de acesso são responsáveis pelo controle do acesso do usuário a um recurso não-público, para tanto toma-se por base na identidade do usuário (serviço de autenticação) bem como no controle do acesso a recursos específicos conforme os privilégios do usuário (conforme o papel que exerce o usuário).
Trata-se de implementação clássica do PDP-PEP em que as informações fornecidas pelo gerenciamento de identidade e acesso são usadas para se determinar a autorização de acesso do usuário.

SDK Security <- implementa o Serviço de Segurança de Controle de Acesso para Mobile conforme o Sistema Operacional utilizado.