draft-perez-abfab-eap-gss-preauth-00

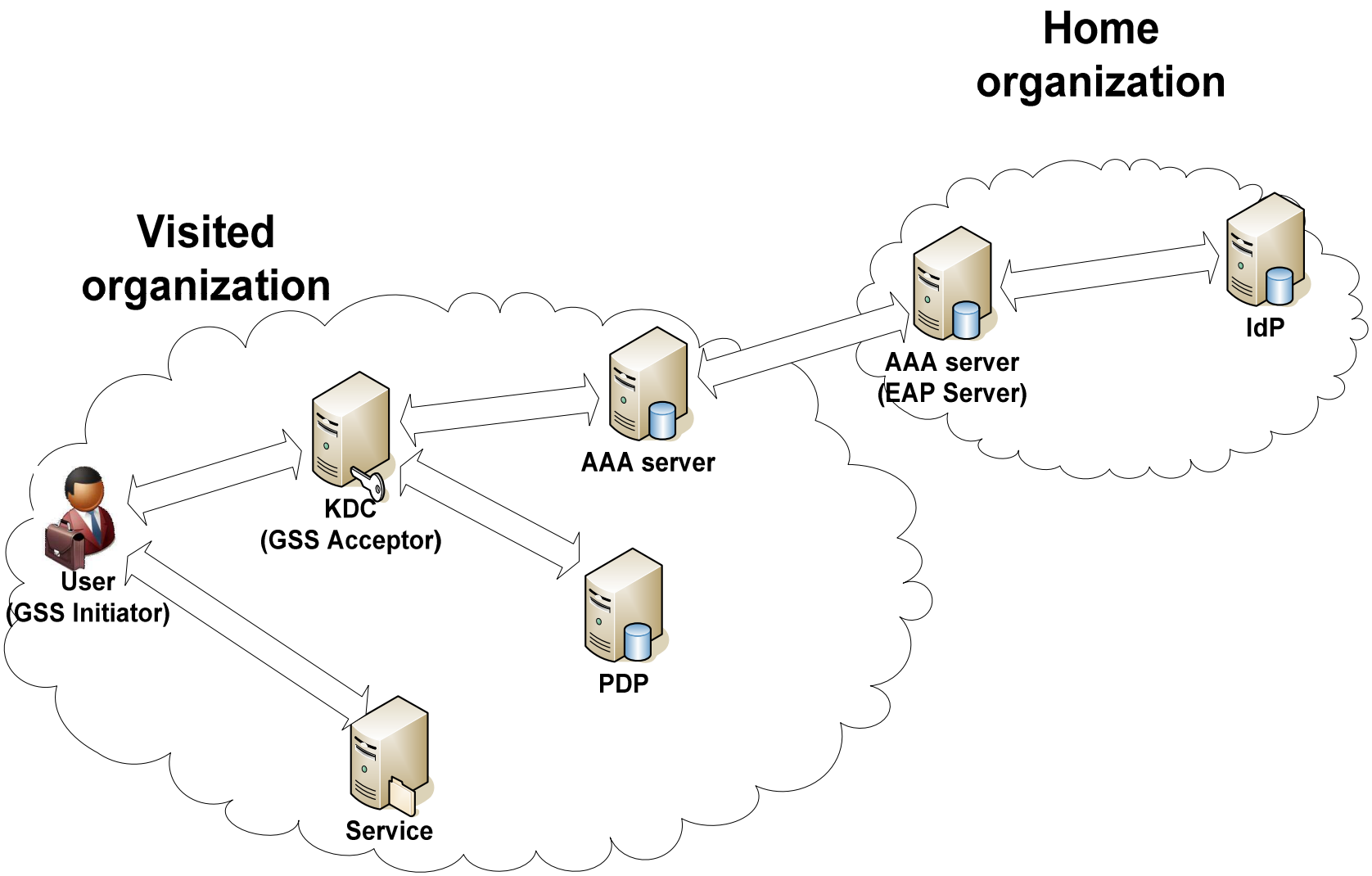
Motivation

- Kerberos has become a widely used authentication and key distribution protocol
  - Supported by most current operating systems and network applications like SSH, FTP, HTTP…
- But typically used in a single-organization scenario
  - Cross-realm infrastructures are not widely deployed
- Instead, organizations deploy AAA federations for controlling service access

Overview

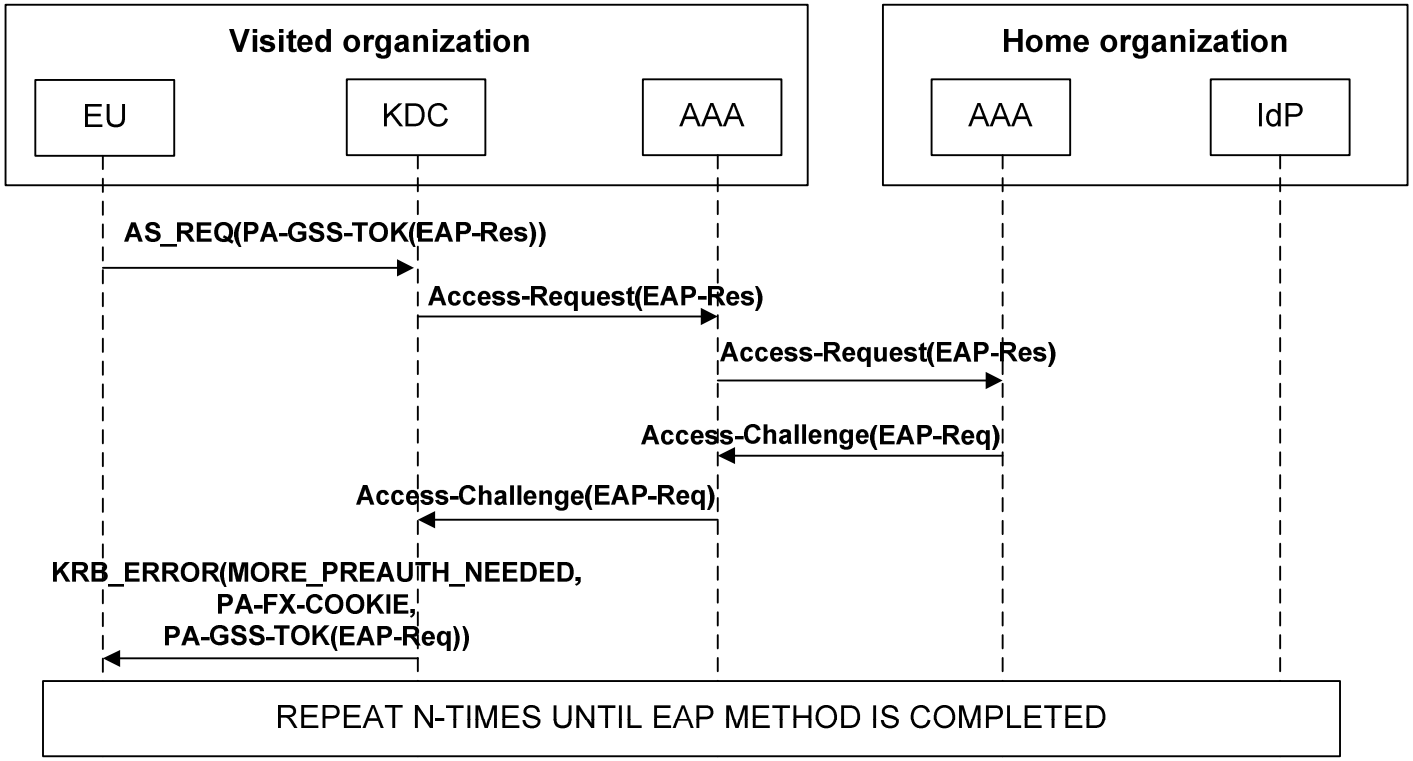
- Integrate the Kerberos infrastructure with the AAA federation
- User performs Kerberos pre-authentication with the KDC based on GSS-EAP mechanism
  - Federated authentication
  - No need for Kerberos cross-realm infrastructures
- KDC obtains SAML Assertion from the user's IdP as a result of the process
  - Assertion is used for authorization → Attributes, validity period, issuer…
- KDC queries a local PDP for an authorization decision
  - It can retrieve additional attributes based on the accessed service
- Process is transparent to deployed services based on Kerberos

Overview


Home
organization
Visited
organization
IdP
AAA server
(EAP Server)
AAA server
KDC
(GSS Acceptor)
User
(GSS Initiator)
PDP
Service

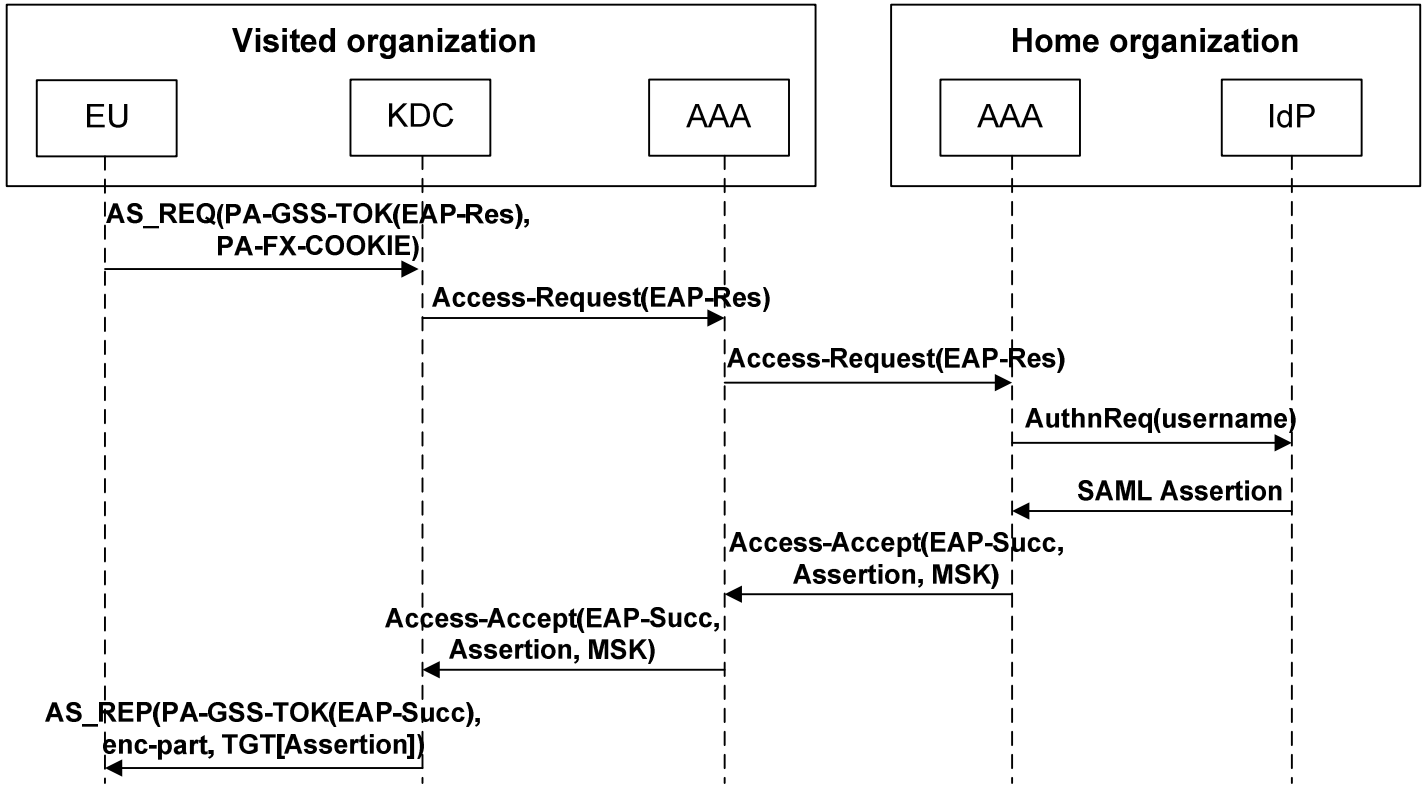
Operation

- User starts pre-authentication with the KDC
  - Pre-authentication based on GSS-EAP, to take advantage of the AAA infrastructure
  - Visited AAA server redirects EAP packets to home domain, based on user's NAI
  - Authentication takes N round-trips



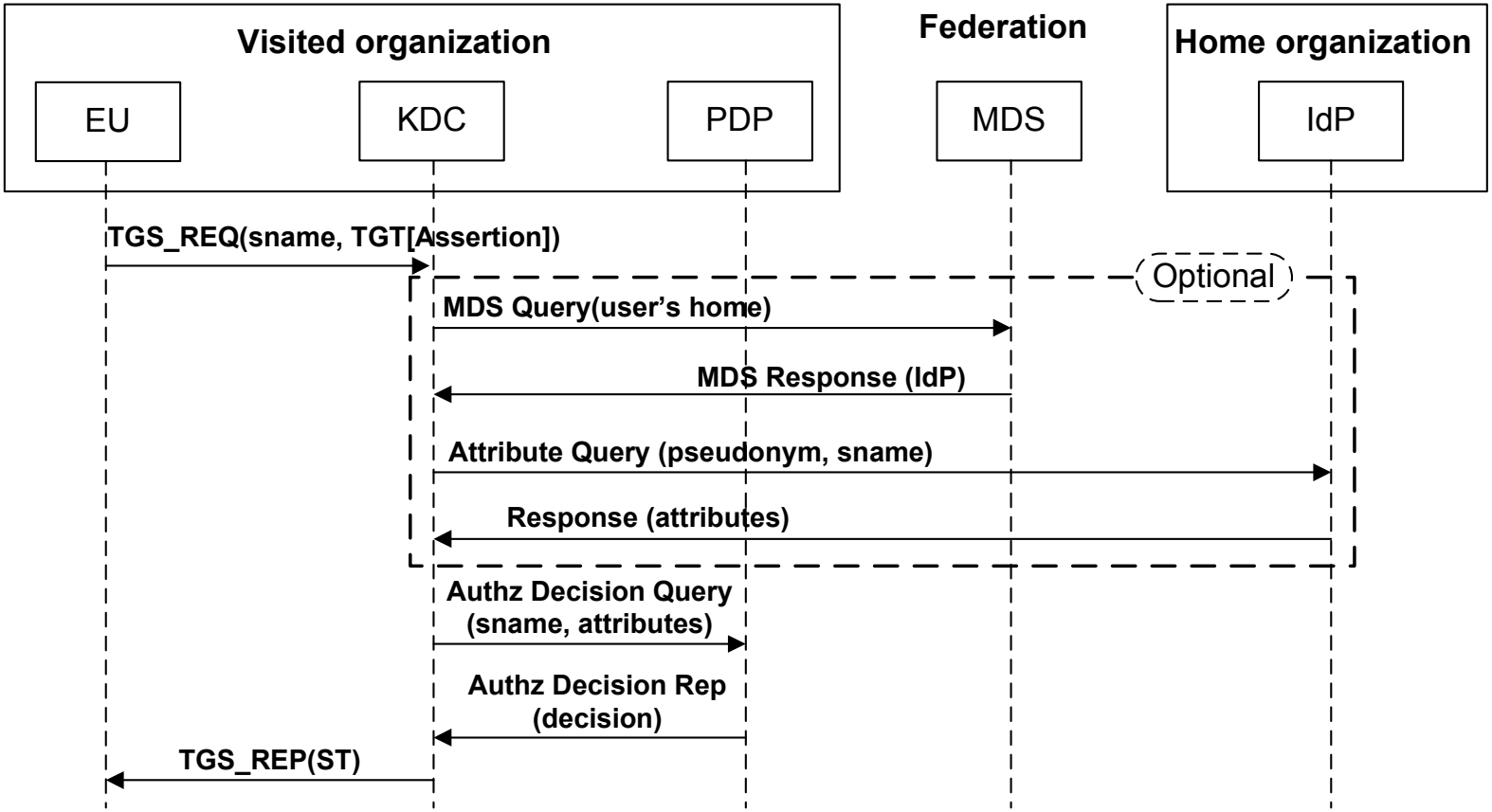
Operation

- Before sending the EAP Success
  - Home AAA server contacts with the home IdP to obtain a SAML Assertion
  - It is sent to the KDC within AAA attributes
- The KDC
  - Derives the *reply key* using *gss_pseudo_random()*
  - Includes the SAML Assertion in the *authorization-data* field of the TGT



Operation

- User requests access to a Kerberized server on the visited organization
  - This triggers the TGS-REQ exchange
  - KCD retrieves user's attributes and queries PDP



Operation

- If user is at his home domain, the process would be similar
  - No difference from the point of view of the KDC or the services