Table of Contents

2 Kerberos in the Cloud: Use Case scenarios

2.1 Definition

The usage of the term Kerberos-in-the-cloud (KITC) in this document is intended to cover a number of configurations of Kerberos being deployed as a service in the cloud.

- *(a) Kerberos authentication service (public)*: In this model, Kerberos authentication is offered as a service by an operator. End-users are able to obtain *global Kerberos identities*, and use the service as Trusted Third Party (TTP) to access other services offered by Relying Parties (RP).
- *(b) Hosted Kerberos service*: In this model, a Hosting Provider offers the necessary environment and management tools to stand-up a Kerberos authentication service. Any entity or person can purchase a hosted-Kerberos service. At least two possible hosted Kerberos service can be conceived:

  (i) *Private Hosted Kerberos Service*: In this mode, the Kerberos authentication service is visible only to entities within the customer's organization (eg. such as an Enterprise). Employees within the Enterprise cannot distinguish between Kerberos operating in this mode from Kerberos operating on a physical server within the perimeter of the Enterprise. All Kerberos identities in this mode is assumed to be locally-scoped.

  (ii) *Public Hosted Kerberos Service*: In the public mode, the Kerberos authentication service is public-facing and end-users can obtain global Kerberos identities. One key difference with configuration (a) is that any entity (not necessarily an operator) can stand-up (or tear-down) this service at the Hosting Provider facilities.

2.2 Background, Assumptions and Requirements

Figure 1 illustrates the Kerberos in the Cloud (KITC) use-cases discussed in the following sections.

Each cloud instance of a Kerberos Key Distribution Center (KDC) is assumed to be front-ended with an Identity Provider (IdP) server that aids in the enrollment of user's identity and credentials. Although the IdP could be easily implemented as a service operating within the KDC, in this document we distinguish these two functions to call out several aspects of the architecture.

- *Enrollment & provisioning*: First, the IdP functions allows the function of user enrollment & provisioning to be separated from the Authentication Server (AS) function within the traditional KDC. Using other standards (e.g. SAML Provisioning), the IdP function becomes the first port of call for new users (employees or customers) seeking to use the Kerberos cloud service.
- *Integration of AS with IdP*: Second, the addition of an IdP function as a front-end to the KDC allows implementers to of the cloud to closely integrate the notion and implementation of tickets as an authentication and authorization mechanism with the the function of the traditional IdP (which typically also contains an authentication capability as well as assertions-generation capability).
- *Flexible end-user authentication*: Thirdly, the use of the IdP as a front-end to the KDC allows the end-user to authenticate to the AS/KDC using other means than the traditional password-over-kerberos approach defined in RFC4120. That is, the IdP function can implement various user

friendly authentication approaches, including password over HTML (over SSL with certs), OTP-tokens, Oauth, Xauth, and others. The act of authenticating the end-user is this distinct from the act of issuing a service-ticket.

- *IdP-to-IdP Interoperability*: The IdP function within the Kerberos Cloud allows easier interoperability of the Kerberos Cloud with Identity Providers in the Internet. In particular, the IdP function allows Kerberos constructs (such as service-tickets) to be wrapped within other structures more familiar to the IdPs (such as SAML assertions).
- *Ticket to token translation*: The Kerberos Cloud may perform the translation of Kerberos service-tickets to other proof-forms, such as OAuth 2.0 Access Tokens, thereby providing a bridge for the end-user to access services/resources offered by Service Providers deploying those tokens.
- *Identity mapping*: The inclusion of an IdP function within the Kerberos Cloud also makes possible the mapping of Kerberos identities (scoped to a Kerberos realm) to other identity forms (such as OpenID format identities). Combined with the ticket-to-token translation capability, the Kerberos Cloud allows the end-user to maintain multiple identities across differing realms, scopes and formats.

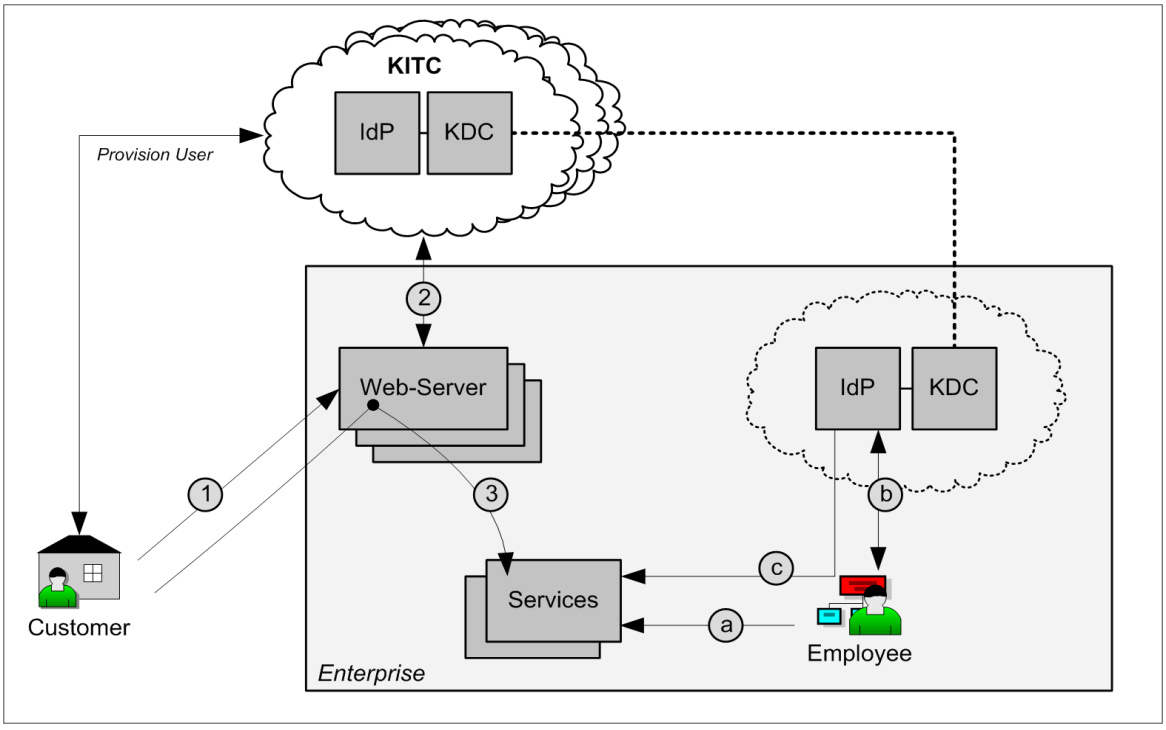

Figure 1

2.3 Use-case #1: Enterprise Private Kerberos Cloud

Many Enterprises seek to move complex tasks into the cloud (private or public) for a number of reasons. These include for providing a more efficient management of the tasks/assets (by the IT Administrators),

for achieving a uniform interface to application developers, and for providing a better user-interface to the end-user.

Figure 1 summarizes the Kerberos authentication service. Following the traditional case, an employee seeking to access Enterprise services and resource must first authenticate to the KDC/IdP in the private to obtain a service-ticket (Steps (a), (b) and (c)).

Figure 1 shows a dotted cloud around the IdP/KDC. This is to indicate that these functions are under the under the administrative control of the Enterprise, but could in fact be operating in a private hosted environment.

2.4 Use-case #2: Enterprise Hosted Kerberos (Semi-Public)

With a mature Kerberos infrastructure as the foundation of employee authentication to services in the Enterprise, there is a desire of many Enterprises to “extend” their Kerberos infrastructure for the purposes of authenticating their own external customers.

Although an Enterprise could create a separate (replicated) Kerberos infrastructure solely for the purposes of customer authentication, a Hosted Kerberos Service would allow an Enterprise to achieve the same degree of compatible authentication quality to their customers without necessarily having to manage a separate infrastructure. Using a hosted configuration, the Enterprise IT Administrators have full (remote) control over the operations of the KDC/IdC (running at the Hosting Provider facilities). The IT Administrator can easily establish cross-realm trust between the two KDCs, as he/she owns both entities in their respective realms. Additionally, the IT administrator can define the scope of the entities to be used in both realms.

Figure 1 shown an external customer enrolled into a KITC service, and obtain his/her Kerberos credentials (Step (0)). The customer then attempts to access resources in the Enterprise and be authenticated by the KITC service (Steps (1) and (2)). Having been issued by the appropriate service-token, the customer then accesses the desired resources (Step (3)).

2.5 Use-case #3: Kerberos Authentication Service (Public)

In this use-case, a Trusted Third Party (TTP) owns and operates a public-facing Kerberos Authentication Service (KAS). Any person or entity can purchase an account with the KAS and use it as the basis for accessing other services offered by a Relying Party (RP). The RP must accept the KAS a legitimate authentication service.

This use-case introduces a number of interesting questions:

- Globally scoped Kerberos names/identities.
- Global realms.
- Global service-tickets.

2.6 Use-case #4: Enrollment & Storing TGTs in the Cloud

TBD.

2.7 Use-case #5: Cross-Cloud Ticket Provisioning

TBD.

2.8 Use-case #6: Ticket-to-Token Translation Service

TBD.