Client-friendly Cross-realm

draft-kamada-krb-client-friendly-cross-03

IETF-71 krb-wg
2008-03-11
KAMADA Ken'ichi
Yokogawa Electric Corporation

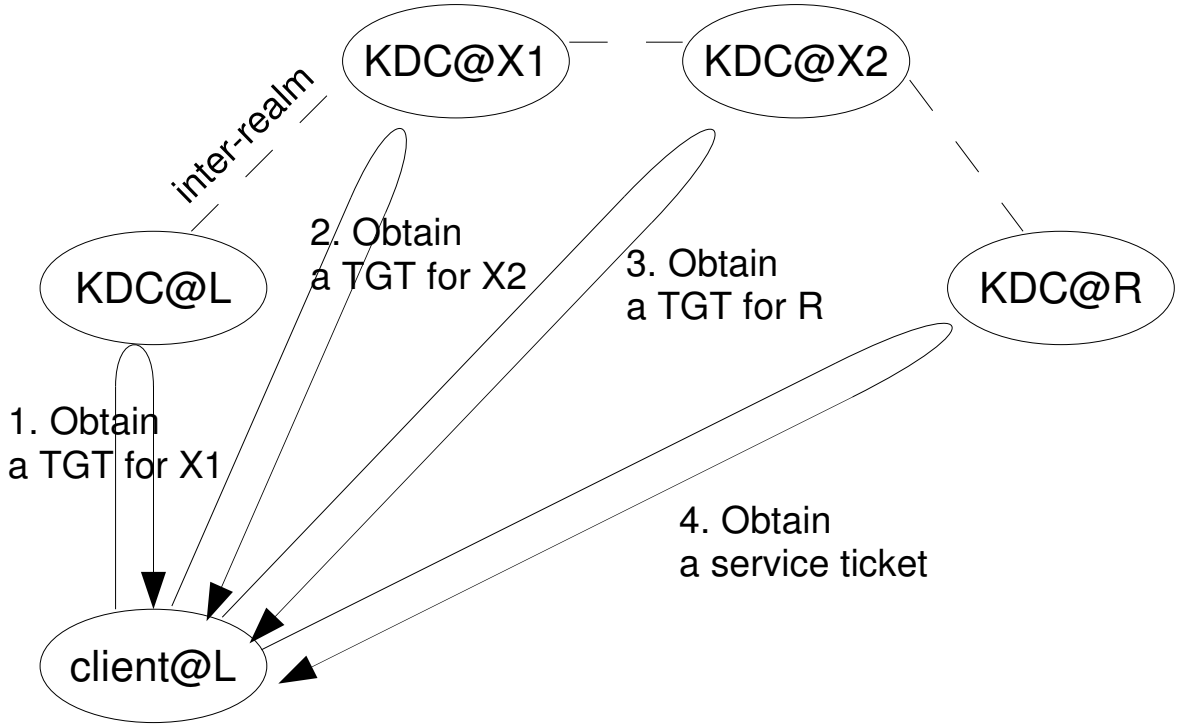
Contents

- Motivation
- Client-friendly cross-realm
  - Recursive Ticketing mode
  - Dynamic Cross mode
- PKCROSS implementation and specification
  - Questions/TODOs

Motivation

- draft-ietf-krb-wg-cross-problem-statement-02 describes several issues on cross-realm.
- The client-friendly cross-realm framework focuses on reducing client workload, while preserving compatibility with existing Kerberos as far as possible.
  - client workload: (Traditional) cross-realm authentication requires a client to contact all the KDCs on the authentication path.
  - The framework may solve some other issues, but that is not the goal but a side effect.

Traditional Cross-realm Operation

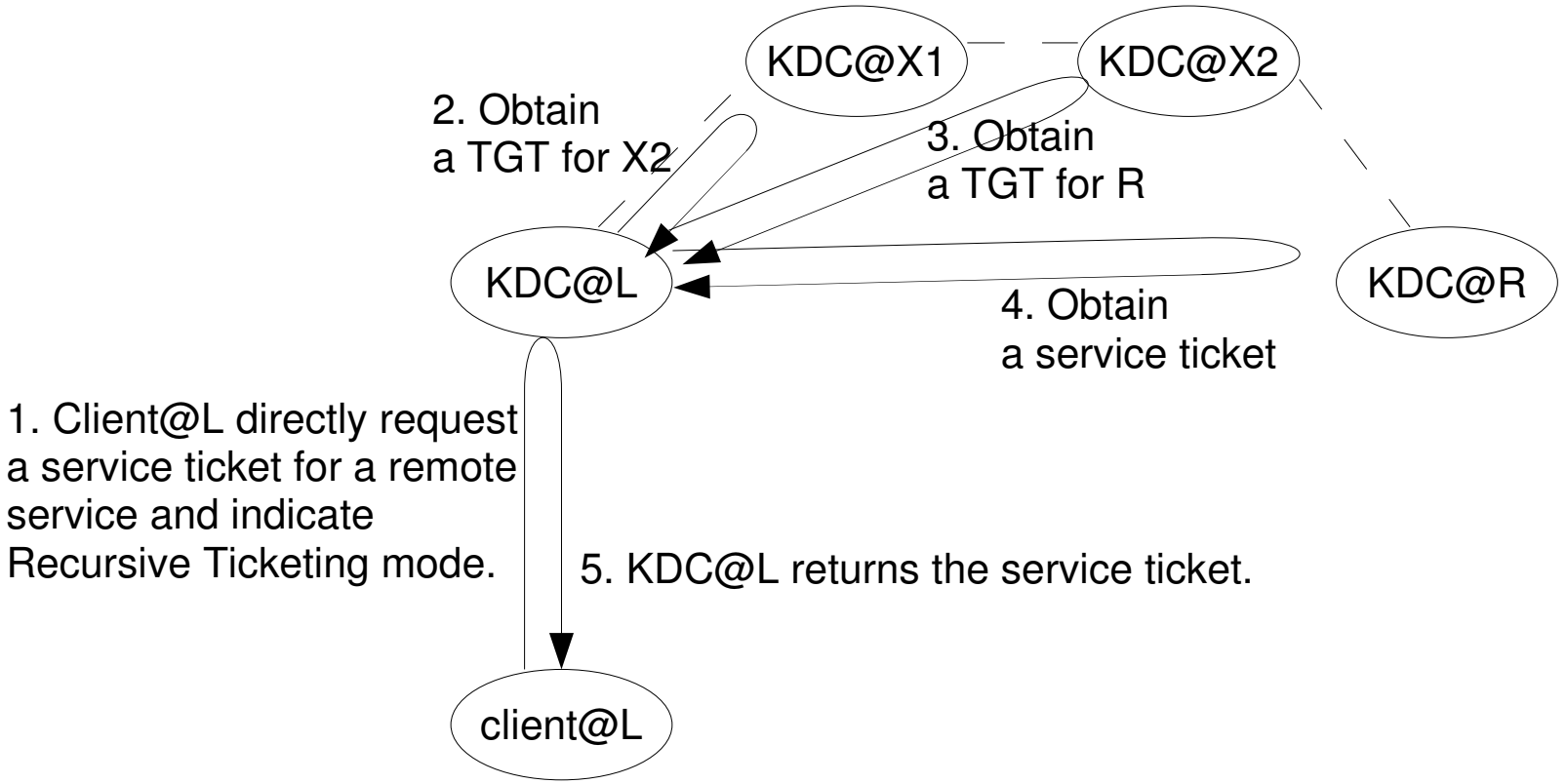


Client-friendly Cross-realm

- draft-kamada-krb-client-friendly-cross-03
- How to reduce the client workload?
  - By delegating the iterative task of traversal to the local KDC -- Recursive Ticketing mode.
  - By caching the result of traversal in the KDC -- Dynamic Cross mode.
    - Generalization of PKCROSS.

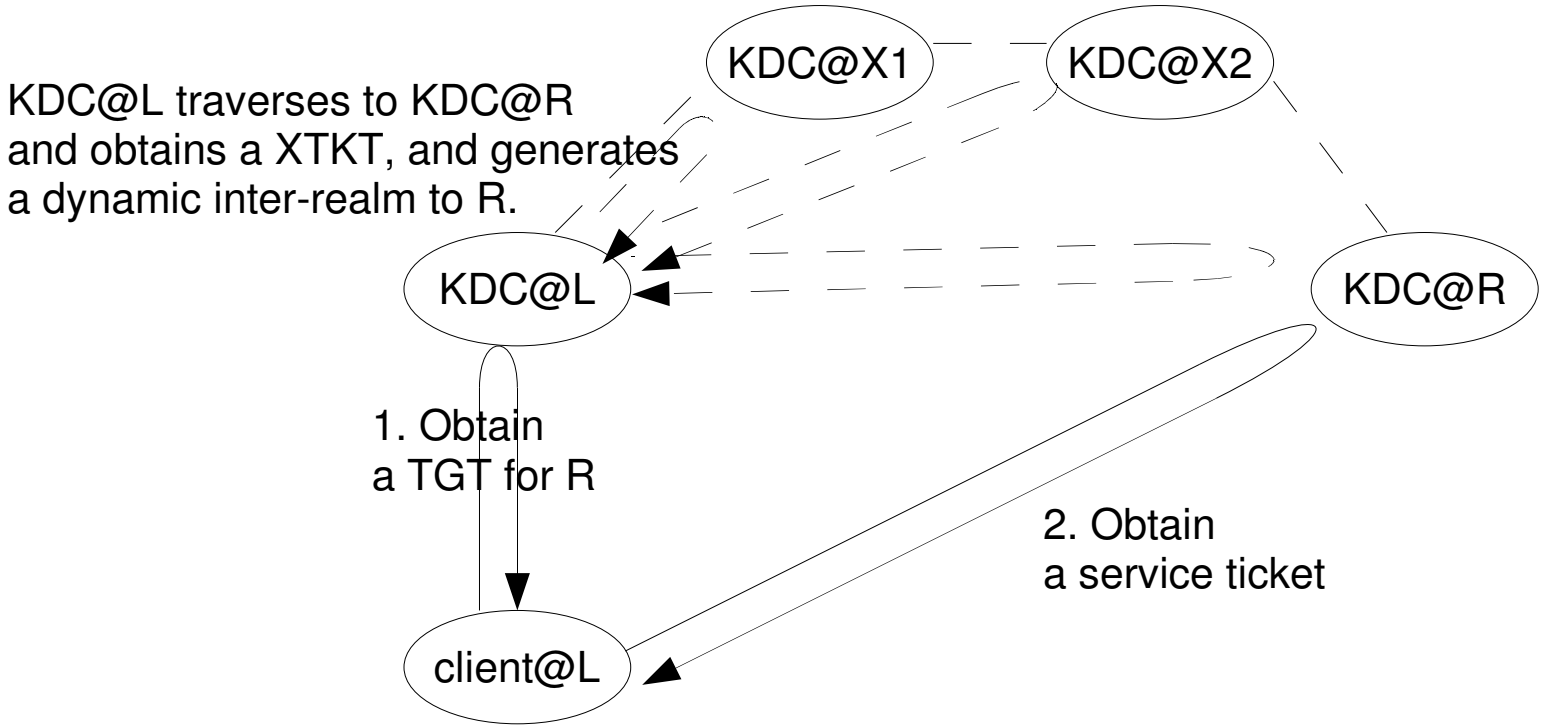
Recursive Ticketing Mode

- The KDC traverses the path ***on behalf of*** the client. (or "impersonate" the client)



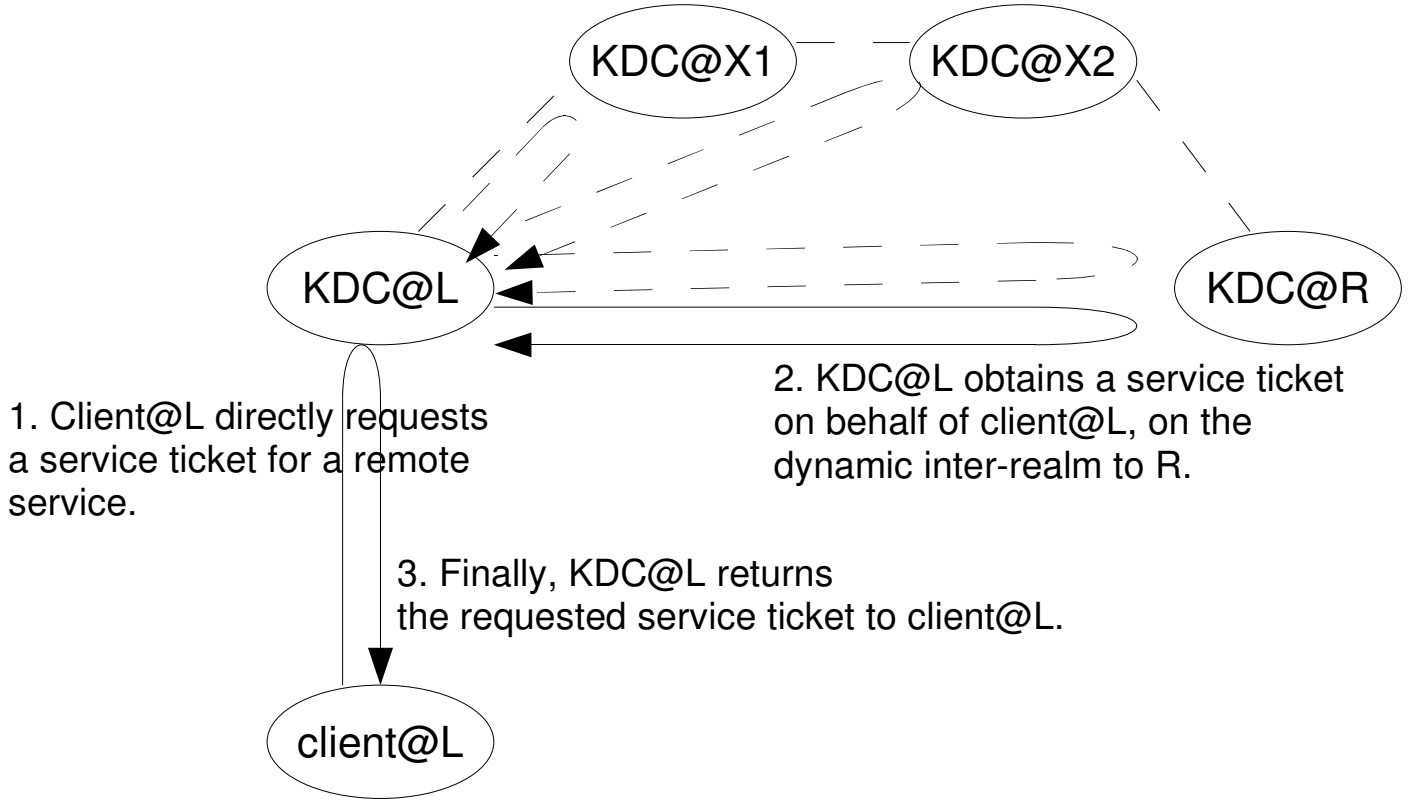
Dynamic Cross Mode

- The KDC ***by itself*** traverses the path (or uses PKINIT) to obtain an inter-KDC ticket. The KDC issues direct cross-realm TGTs using the session key of the inter-KDC ticket.



From the client point of view, the realms L and R seem to have a direct inter-realm.

Both Modes Can be Combined



PKCROSS Implementation

- We have implemented PKCROSS.
  - as an instance of Dynamic Cross mode.
  - based on Heimdal 1.0.1.
- Still rough, but have basic features working.
  - Upon a request from a client, the local KDC can
    - suspend the request,
    - conduct PKINIT with the remote KDC, and
    - resume the processing of the request.
  - etype-based Ticket Extensions
    - XTKT with CrossRealmTktData
    - cross-realm TGT with XTKT

PKCROSS Spec. (from Impl.)

- Questions/TODOs
  - etype negotiation -- needs spec.
    - The local KDC does not know which etypes the remote KDC supports.
  - When can XTKT be issues safely?
    - Can it be issued to anyone?
  - How to verify a cross-realm TGT with XTKT?
    - (or how to verify the peer is a KDC of the realm?)
  - etype-based ticket extensions
    - We are simply embedding typed holes for now. -- need checksum?
- We'd like to feedback to the spec.

Summarizing Cross-realm Activities

- http://www.taca.jp/krb-cross-realm/
  - The PKCROSS implementation will be also available here.