Inter-KDC protocol for improved Kerberos cross-realm operations

Issues in Kerberos cross-realm operations

**Definitions**
- **Key Distribution Center (KDC):**
  - Shares keys with clients, services, other KDCs
  - Has two components: AS, TGS
- **Ticket Granting Ticket (TGT):**
  - Obtained by clients from the AS
  - Allows clients to communicate with TGS
- **Service Ticket (ST):**
  - Obtained by clients (who have a TGT) from the TGS
  - Allows clients to communicate with an application svc

**Operations**
1 : C -> TGS-H : Give me TGT for TGS-R
TGS-H -> C : TGT for TGS-I/1
2,3 : C -> TGS-I/n : Give me TGT for TGS-R
TGS-I/n -> C : TGT for TGS-I/n+1
4 : C -> TGS-I/3 : Give me TGT for TGS-R
TGS-I/3 -> C : TGT for TGS-R
5 : C -> TGS-R : Give me ST for SVC-R
TGS-R -> C : ST for SVC-R
6 : C authenticates with SVC-R

Issues

**Performance**
- Client involved in too many exchanges
  - Not adapted for small devices

**Reliability**
- If any Intermediary KDC is down
  - Client can’t authenticate

**Security**
- If any Intermediary KDC is corrupted
  - Client/server communication unsafe

Our approach : XTGSP, the inter-TGS Kerberos cross-realm protocol

**Concept**
- No Intermediary KDCs
- Public-Key cryptography to establish Inter-realm trust
- Client requests an ST for SVC-R from its home KDC
- Home KDC communicates with remote KDC to build a ST for the client

**Operations**
1 : C -> TGS-H : Give me ST for SVC-R
2 : TGS-H -> TGS-R : Give me a ST for my client C to access your service SVC-R.
3 : TGS-R -> TGS-H : Here is a ST
4 : C -> TGS-H : ST for SVC-R
5 : C authenticates with SVC-R

Advantages

- Cross-realm processing delegated to KDCs
- Less load on small devices
- No intermediary KDCs
- Better reliability, better security