Changes Since 00

- Defined name format for GSS-EAP names
- Defined requirements for EAP mechanisms
- Defined interactions with channel binding
NAME FORMAT

- Mostly compatible with Kerberos
- Compatible with NAI for usernames

```
service-specifics = service-specific 0*(’/’ service-specifics)
name = user-or-service ’/’ host [ ’/’ service-specifics] [ ’@’ realm ]
```
Dictionary attack resistance always required
When per-message services are requested key derivation is required.
When mutual authentication is requested:
   - Mutual auth is required
   - Channel binding is required
Changes Required

- Empty target_name
- Server name indication
- Requirement: extensible tokens
Proposed Solution

- TLV encoding for each token
- State machine manages what tokens are allowed at each state
- Tokens to send acceptor names
Requirement for MIC

→ Should we have integrity protection over the entire exchange
→ If so, problematic for partial contexts and constrained clients
→ Extension requiring protection: GSS flags to acceptor