Features of DAC-MACS

All key security requirements of Bdrive are fulfilled.

- **(efficient) Direct Revocation**
  - forward security
  - backward security
- **efficient decryption**
  - by doing the main work on the server
- **Multi-Authority CP-ABE**
- **CA (Certificate Authority)**
  - does not have global decryption power
  - must be trusted
- **Server**
  - semi-trusted
  - serves as proxy worker for clients
  - helps user by decryption and cipher text updates
    - user provides his AA secret keys to the server
    - server does not know the plain text since it is encrypted with the users global public key
- **Collusion resistance**
  - using UIDs that are user dependent
- **Large key universe**
  - de- and encryption scales linearly with the number of attributes and authorities
  - revoking attributes only affects the cipher text and keys that are associated with the revoked attributes
- **Adding new Attribute Authorities**
  - possible since we have independent encryption keys for each attribute authority
- **Master key**
  - decryption power is AA domain intern
- **End-to-end encryption**
  - Might be archived by either decrypt the cipher text on the client or
  - self create private/public key pair so that only the public component is known to the CA
    - However, we need to make sure that than the users do not collude (for example some kind of Diffie-Hellman key exchange mechanism?)
- **Certificates**
  - users public key parameter and UID are protected by certificates of the CA

Weaknesses:

- Traitor tracing
  - is an optional requirement
- One key per cipher text
  - To act dynamically on adding new AAs we need to encrypt for each AA separately
- Scalable decryption
  - questionable since the main work for decryption is done on the server
  - this scales linearly with the number of attribute involved in the cipher text
  - thread of DoS attack