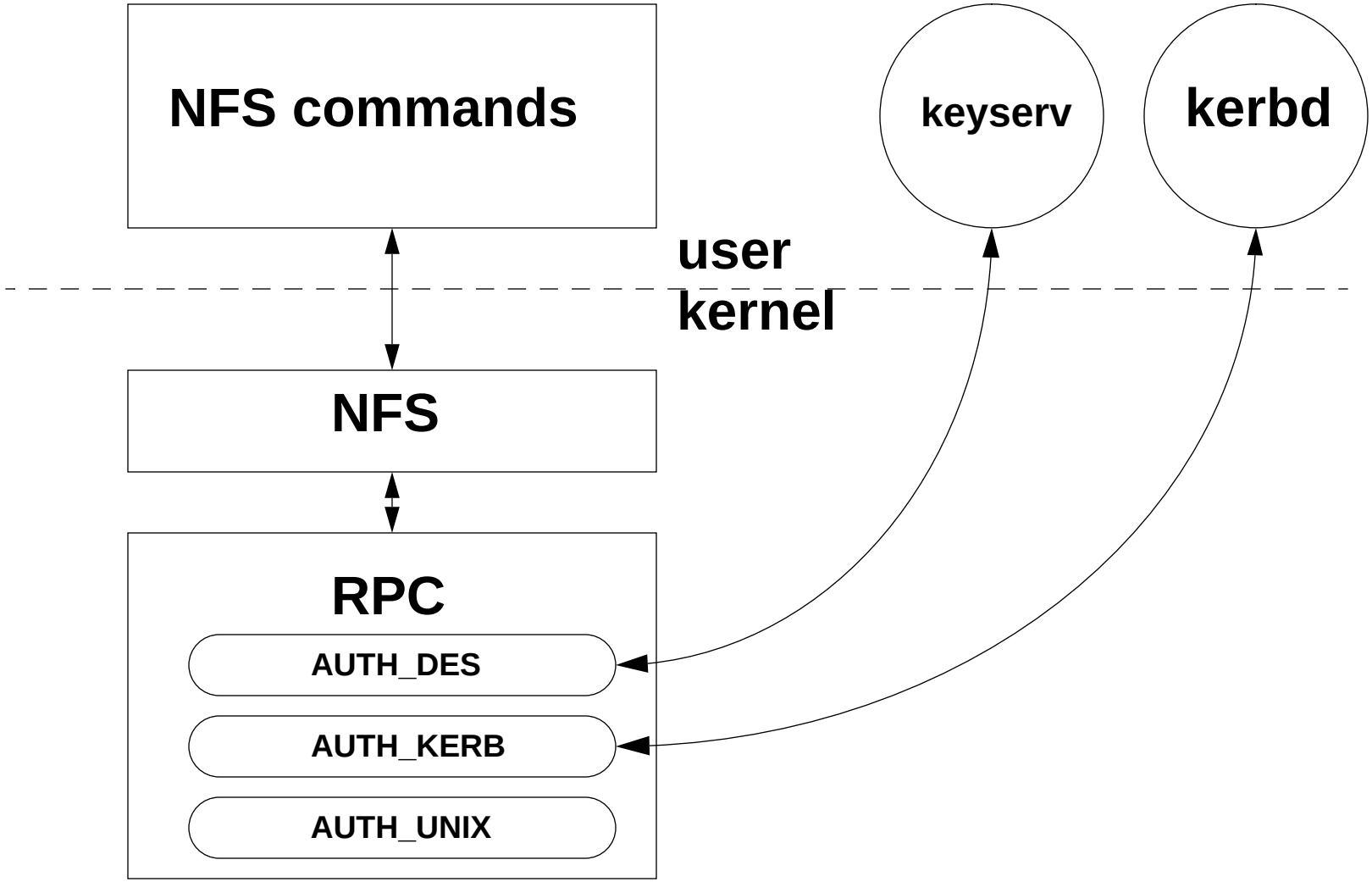
NFS and RPCSEC_GSS

- AUTH_UNIX
- AUTH_DES
- AUTH_KERB
- *RPCSEC_GSS*

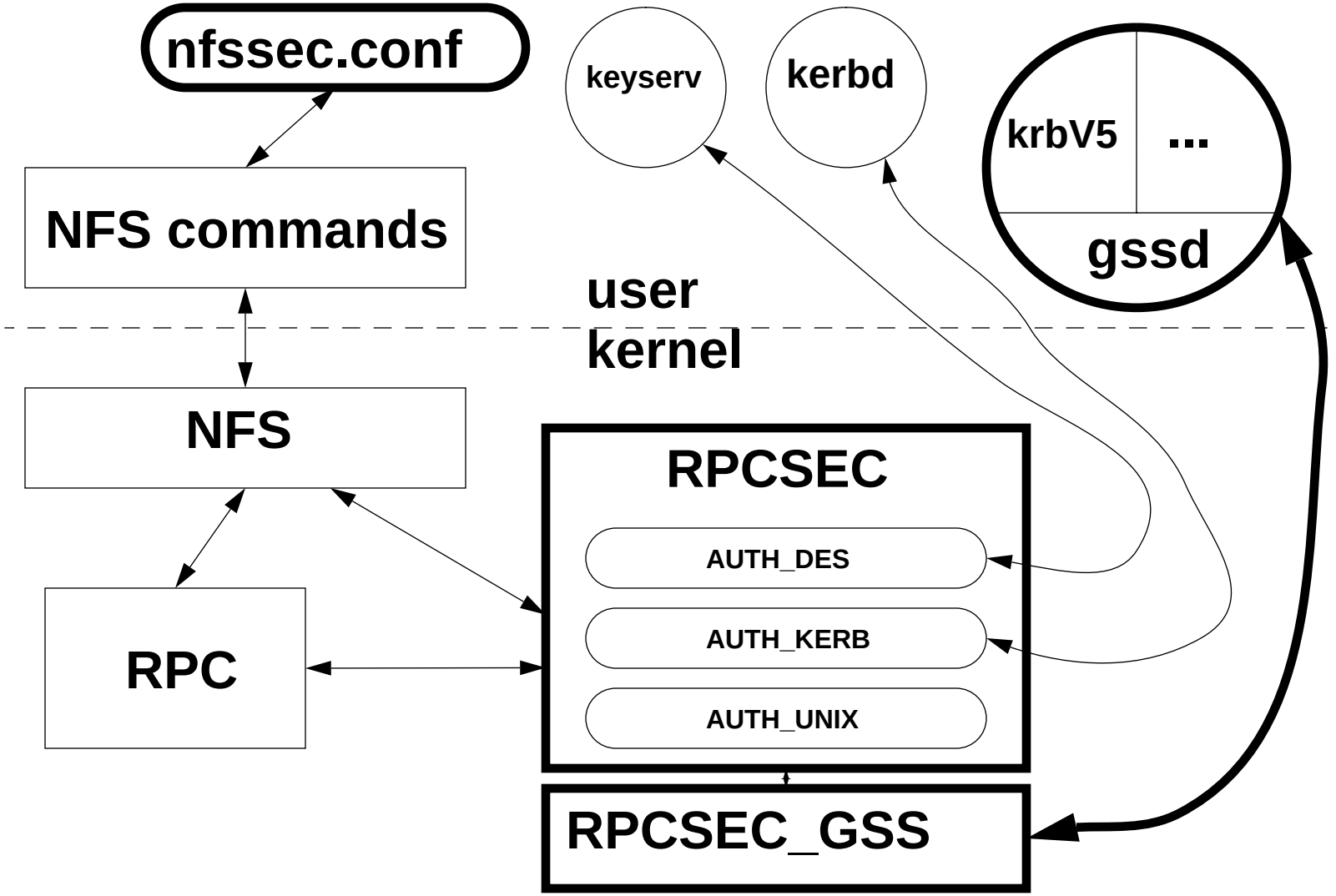
Why RPCSEC_GSS

- **Security mechanism independence**
- **Services beyond authentication**
  - integrity
  - privacy
- **Use standards where they exist**

CURRENT SECURITY FRAMEWORK



FRAMEWORK FOR RPCSEC_GSS



RPC vs MOUNT Flavor Numbers

- **MOUNT V3 has a simple array of flavor numbers for flavor negotiation.**
- **An RPCSEC_GSS session bound to a specific triple of:**
  - mechanism, quality_of_protection, service
- **NFS servers want to bind exported file system to RPCSEC_GSS triplets.**
- **Too late for a MOUNT protocol change**

RPC vs MOUNT Flavor Numbers

- **Solution : we map RPCSEC_GSS triplets to pseudo flavors via /etc/nfssec.conf**

RPC flavor	MOUNT flavor
AUTH_UNIX	AUTH_UNIX
AUTH_DES	AUTH_DES
AUTH_KERB	AUTH_KERB

RPCSEC_GSS triplets	MOUNT flavor
krb5, md5-des, integrity	flavor X
krb5, md5-des, privacy	flavor Y

PROTOTYPE

- **First mechanism - Kerberos V5 (RFC 1510)**
- **/etc/nfssec.conf**

<nfs_flavor_name>	<nfs_flavor_num>	<gss_mechanism>	<gss_qop>	<gss_svc>
unix	1	-	-	-
des	3	-	-	-
krb4	4	-	-	-
krb5	5	kerberos_v5	-	none
krb5i	6	kerberos_v5	-	integrity
krb5p	7	kerberos_v5	-	privacy

- **share -o sec=krb5i:krb5p /export**

• mount -o sec=krb5p

RPC: ----- SUN RPC Header -----
RPC:
RPC: Transaction id = 853156479
RPC: Type = 0 **(Call)**
RPC: RPC version = 2
RPC: Program = 100003 (NFS), version = 3, procedure = 0
RPC: Credentials: **Flavor = 15 (RPCSEC_GSS)**, len = 20 bytes
RPC: version = 1
RPC: gss control procedure = 1 (RPCSEC_GSS_INIT)
RPC: sequence num = 0
RPC: service = 3 (privacy)
RPC: handle: length = 0, data = []
RPC: Verifier : Flavor = 0 (None), len = 0 bytes
RPC:
RPC: **RPCSEC_GSS_INIT args:**
RPC: **gss token: length = 480, data = [480 bytes]**
RPC: **quality of protection (qop) = 0**
RPC: **service = 3 (privacy)**

RPC: ----- SUN RPC Header -----
RPC: Transaction id = 853156479
RPC: Type = 1 **(Reply)**
RPC: This is a reply to frame 32
RPC: Status = 0 **(Accepted)**
RPC: Verifier : Flavor = 0 (None), len = 0 bytes
RPC: Accept status = 0 (Success)
RPC:
RPC: RPCSEC_GSS_INIT result:
RPC: handle: length = 4, data = [00000001]
RPC: gss_major status = 0
RPC: gss_minor status = 0
RPC: sequence window = 128
RPC: gss token: length = 102, data = [102 bytes]
RPC:

RPC: ----- SUN RPC Header -----
RPC:
RPC: Transaction id = 853156479
RPC: Type = 0 **(Call)**
RPC: RPC version = 2
RPC: Program = 100003 (NFS), version = 3, procedure = 19
RPC: Credentials: **Flavor = 15 (RPCSEC_GSS)**, len = 24 bytes
RPC: version = 1
RPC: gss control procedure = 0 (RPCSEC_GSS_NULL)
RPC: sequence num = 2
RPC: service = 3 **(privacy)**
RPC: handle: length = 4, data = [00000001]
RPC: Verifier : Flavor = 15 (RPCSEC_GSS), len = 33 bytes
RPC: [601F06052B0501050201010000FFFFFFFF2CDF2ABA31F3D92685255974FAB5C194]
RPC:
RPC: **RPCSEC_GSS NFS ver(3) proc(19) (CALL args encrypted)**
RPC:

RPC: ----- SUN RPC Header -----
RPC:
RPC: Transaction id = 853156479
RPC: Type = 1 **(Reply)**
RPC: This is a reply to frame 32
RPC: Status = 0 (Accepted)
RPC: Verifier : Flavor = 15 (RPCSEC_GSS), len = 33 bytes
RPC: [601F06052B0501050201010000FFFFFFFF08B650A4EF82159E58FFBCF7D8F89F87]
RPC: Accept status = 0 (Success)
RPC:
RPC: **RPCSEC_GSS NFS ver(3) proc(19) (REPLY args encrypted)**
RPC: