Where do you store Digital Certificates on your production systems?

Responses	Count	Percent %
RACF (ICSF or other hardware protected store)	12	33.3%
RACF (database)	33	91.7%
Unix files created with gskkyman	3	8.3%
Unix files created with PKI Services	1	2.8%
Responses	**36**	
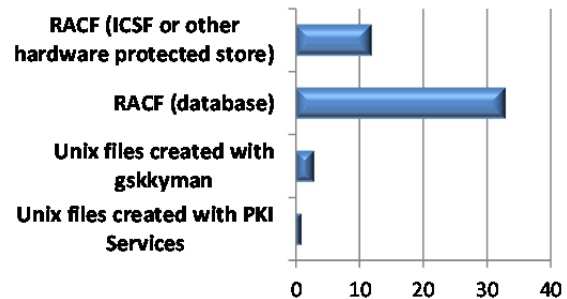
Approximately how many keyrings do you have on your production systems?

| Number Range	Count	Percent %
None	0	0.0%
Less than 10	18	50.0%
10 to 25	14	38.9%
Over 25	4	11.1%
Total	**36**	**100%**
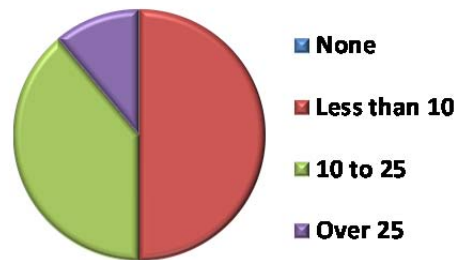
Which of the following most closely matches how often do you search for near-expiration production certificates?

Responses	Count	Percent %
Once a day	4	11.1%
Once per week	7	19.4%
Once per month	10	27.8%
Once per sixty days	0	0.0%
Once per quarter	1	2.8%
Once per six months	3	8.3%
Once per year	6	16.7%
Never	5	13.9%
Total	**36**	**100%**
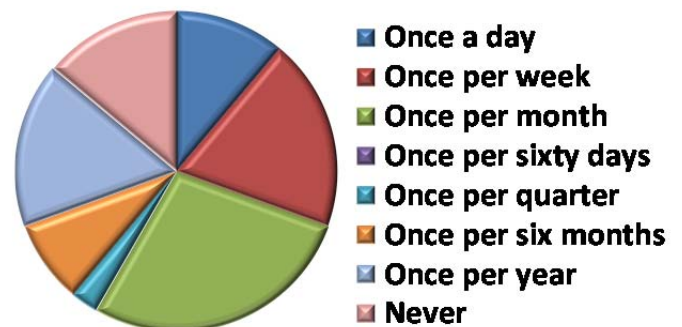
How do you search for near-expiration production certificates?

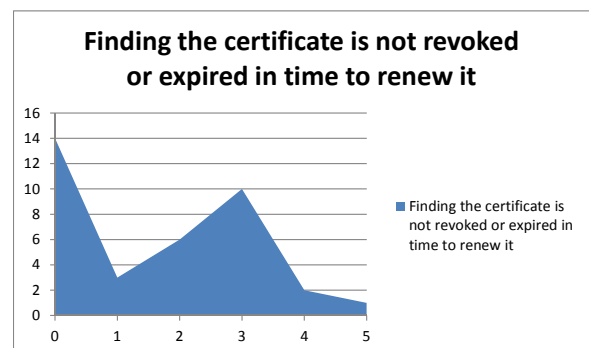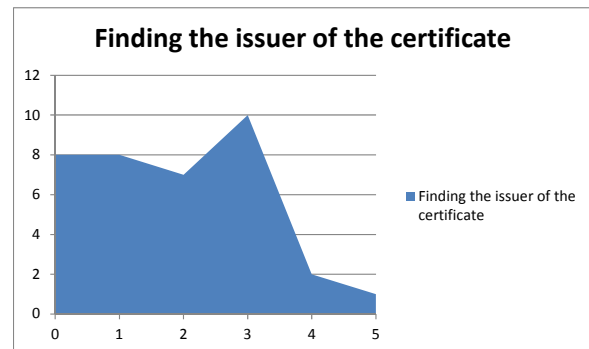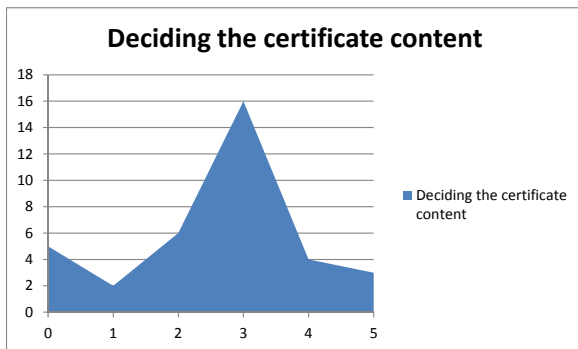| Responses	Count	Percent %
RACDCERT LIST (for RACF-managed certificates)	12	33.3%
Unloaded copy of the RACF database	9	25.0%
RACF_CERTIFICATE_EXPIRATION health check (V2.1 only)	0	0.0%
PKI Services web interface to perform a query	1	2.8%
RACF administration add-on product	15	41.7%
List commands associated with the key store (non-RACF certificates)	2	5.6%
Other:	10	27.8%
- manually maintained list - 2 - dkms - Access DB + home-made Rexx using RACDCERT - Manually, and monthly check with TWS-REXX-Job - Wait for them to expire, then fix - DB2 query - Locally developed tool to search RACF - Report from RACF database info loaded into DB2 - Own Rexx routine which interprets and send mail based on RACDCERT LIST		
Responses	**36**	
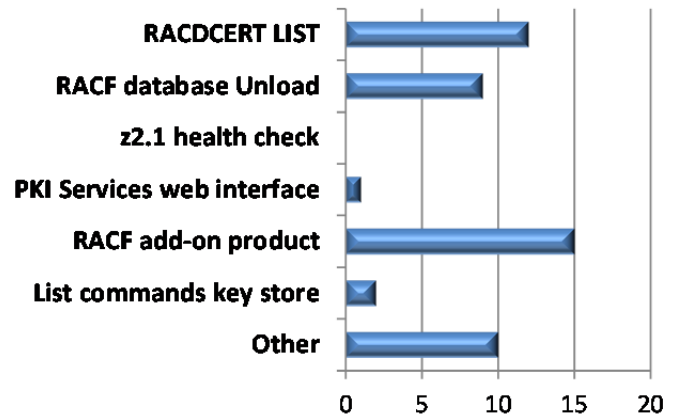
How do you use the RACDCERT command?

Responses	Count	Percent %
Do not use it	1	2.8%
Generate complete key pair plus certificate (single GENCERT)	30	83.3%
Generate Certificate Signing Request (CSR)	25	69.4%
Process and sign a CSR to produce a public certificate	15	41.7%
Import complete PKCS12	21	58.3%
Export complete PKCS12	13	36.1%
Other:	1	2.8%
- renew certificates; maintain ICSF tokens, key rings and mappings		
Responses	**36**	
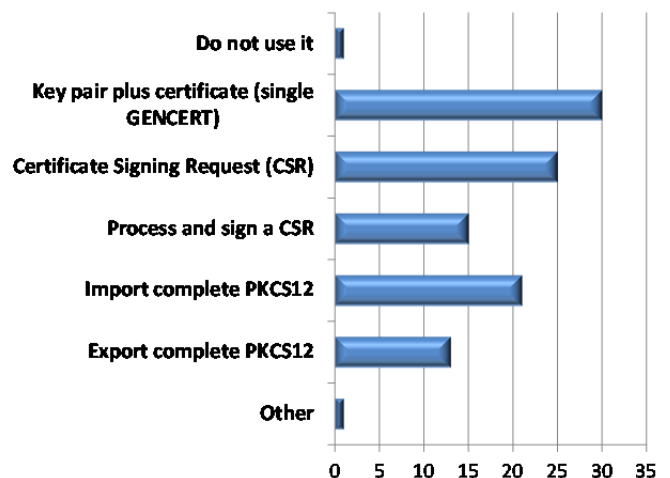
Rate the following steps in certificate management on a scale of 0 (easy) to 5 (difficult).

Responses	0	1	2	3	4	5
Deciding the certificate content	5	2	6	16	4	3
Finding the issuer of the certificate	8	8	7	10	2	1
Deciding what certificates needed to be in the key store	4	9	4	11	6	2
Finding the certificate is not revoked or expired in time to renew it	14	3	6	10	2	1
Responses	36					

Deciding the certificate content

Finding the issuer of the certificate

Deciding what certificates needed to be in the key store

Finding the certificate is not revoked or expired in time to renew it