Likevel er det ikke hensiktsmessig å disponere kravtabellene i en standard etter ulike mål som skal avveies mot hverandre. Den funksjonsorienterte inndelingen av sikkerhetsegenskaper i dette kapitlet forutsetter at hvert organ som skal bruke en Noark 5-løsning *på forhånd* har besluttet sin egen sikkerhetspolicy. Sikkerhetspolicyen vil være basert på de regelverk organet er underlagt, og på organets avveininger mellom behov for konfidensialitet, integritet og tilgjengelighet.

12.1.2 Terminologi: Sikkerhetsfunksjoner og -egenskaper

Kravene i dette kapitlet angir i all hovedsak *sikkerhetsfunksjoner*. En eller flere sikkerhetsfunksjoner kan ivareta forskjellige *sikkerhetsegenskaper*, som kan være implisitte eller eksplisitte. Sikkerhetsfunksjonene kan også være til dels overlappende, ved at flere forskjellige funksjoner kan ivareta samme sikkerhetsegenskap.

Et eksempel som belyser begrepsbruken: "Pålogging med passord" er en *funksjon*, som primært skal ivareta den *egenskapen* at brukeren må være autentisert for å få tilgang til systemet.[19] "Pålogging med smartkort og PIN-kode" ville være en annen variant av sikkerhetsfunksjonen pålogging. Den ivaretar samme egenskap (autentisering), men i sterkere grad.

12.2 Kontroll med tilgang til informasjon

12.2.1 Identifisering av brukere

For alle eksterne løsninger som skal integreres med Noark 5 kjernen, må brukerne av den eksterne løsningen være individuelt og entydig identifisert og pålogget. Påloggingen kan enten være validert i den aktuelle eksterne løsningen, eller i en integrert, ekstern sikkerhetsløsning. For enkel integrasjon og helhetlig sikkerhetspolicy på tvers av virksomhetenes IT-systemer anbefales generelt sikkerhetsfunksjoner som legger til rette for brukerkataloger utenfor Noark 5-løsningen.

Krav nr.	Krav til identifisering av brukere	Type	Merknad
12.2.1	Alle brukere som skal ha tilgang til Noark 5-løsningen må være individuelt identifisert, og autentisert i tilstrekkelig grad	O	
12.2.2	Ekstern katalog over identifiserte brukere kan brukes, i stedet for eksplisitt pålogging til Noark 5-løsningen	V	
12.2.3	Brukeren kan være pålogget en tilknyttet ekstern løsning, og la den eksterne løsningen ta hånd om hvilke rettigheter brukeren skal ha	V	
12.2.4	Brukeren kan være pålogget i løsningens driftsmiljø, og ha definert tilgangsrettigheter i en ressurskatalog. Noark 5-løsningen kan da brukes så langt de eksternt definerte tilgangsrettighetene rekker ("single sign-on")	V	

[19] Innen informasjonssikkerhet betyr autentisering at en bruker (eller en elektronisk tjeneste) kan godtgjøre at vedkommende er den han gir seg ut for å være, for eksempel ved pålogging. I arkivfaglig sammenheng brukes begrepet autentisitet vanligvis om arkivmaterialets ekthet.