	Sicherheit auf der Netzwerkschicht		Sicherheit auf der Anwendungsschicht		
	IPSec und VPN	Firewalls	GSI	CAS	Permis
Vertrau-lichkeit	Keine Manipulation von Daten möglich. Datenverkehr nur für Autorisierte benutzer möglich.	Keinen direkten Einfluss in Datenverkehr.	Vertraulichkeit der Daten wird durch Verwendung der asymmetrischen Kryptographie geschützt	Werden nach Authentifizierung über Proxy-Zertifikat geschützt. Anfragen erfolgen nur über die Proxy Credentials.	Vertraulichkeit wird mit den Attribut Zertifikaten geschützt
Authenti-fizierung	Authentifizierung mithilfe von Protokollen wie Authentication Header (AH), Encapsulated Secuirty Payload (ESP) sowie Internet Key Exchange (IKE).	Authentifizierung nur bei speziellen Anwendungsfällen relevant.	Authetifizierung erfolgt über die die Zertifikate	Ein Benutzer kann über das Proxy-Zertifikat authetifiziert werden	Erfolgt über Distinguished Name des Attribut-Zertifikats.
Integrität	Integrität durch Verschlüsselung der Daten sichergestellt.	Integrität der Daten ist keine direkte Aufgabe einer Firewall.	Integrität der Daten wird durch Verwendung der asymmetrischen Kryptographie geschützt	Datenintegriät ist über das Proxy-Zertifikat gegeben	Integrität ist über Attribut Zertifikat gegeben
Nicht-Anfechtbar-keit	Nicht-Anfechtbarkeit der Daten ist indirekt durch die Integrität sichergestellt. Ein Mechanismus zur sicherherstellung kann das Logging des Internettraffics sein.	Die Nicht-Anfechtbarkeit ist durch die Einbindung der Firewall-Logs in den Security Workflow der Organisation sichergestellt.	Nicht-Anfechtbarkeit ist über die Public-Key-Infrastructure gegeben.	Nicht-Anfechtbarkeit ist über Proxy-Zertifikat gegeben	Nicht-Anfechtbarkeit ist über Attribut Zertifikat gegeben
Zugriffs-steuerung/ Autorisierung	Die Verbindung mittels VPN ist nur Berechtigten Personen möglich, die über die entsprechenden Anmeldeinformatio nen verfügen.	Schränkt den Datenverkehr durch Security Policies ein. Ist dadurch ein zentrales Glied in der Zugriffssteuerung.	Erfolgt über die Access Controll Lists	Autorisierung erfolgt über die Richtlinien der Webseite und Gemeinschaft. Die Infromationen befinden sich im Proxy-Zertifikat	Authorisierung erfolgt über den Server und die dort definierten Autorisierungsri chtlinien
Verfügbarkeit	Die Vefügbarkeit kann nur indirekt durch die Verwendung von VPN sichergestellt werden.	Durch DDOS Protection und andere Mechanismen stellt die Firewall die Verfügbarkeit der dahinter liegenden Infrastruktur sicher.	Keine näheren Infromationen	CAS Serve muss zusätzlich geschützt werden. Fällt er aus, funktioniert das System nicht.	Server, der alle Attribut-Zertifikate hostet muss zusätzlich geschützt werden. Fällt er aus, funktioniert das System nicht.