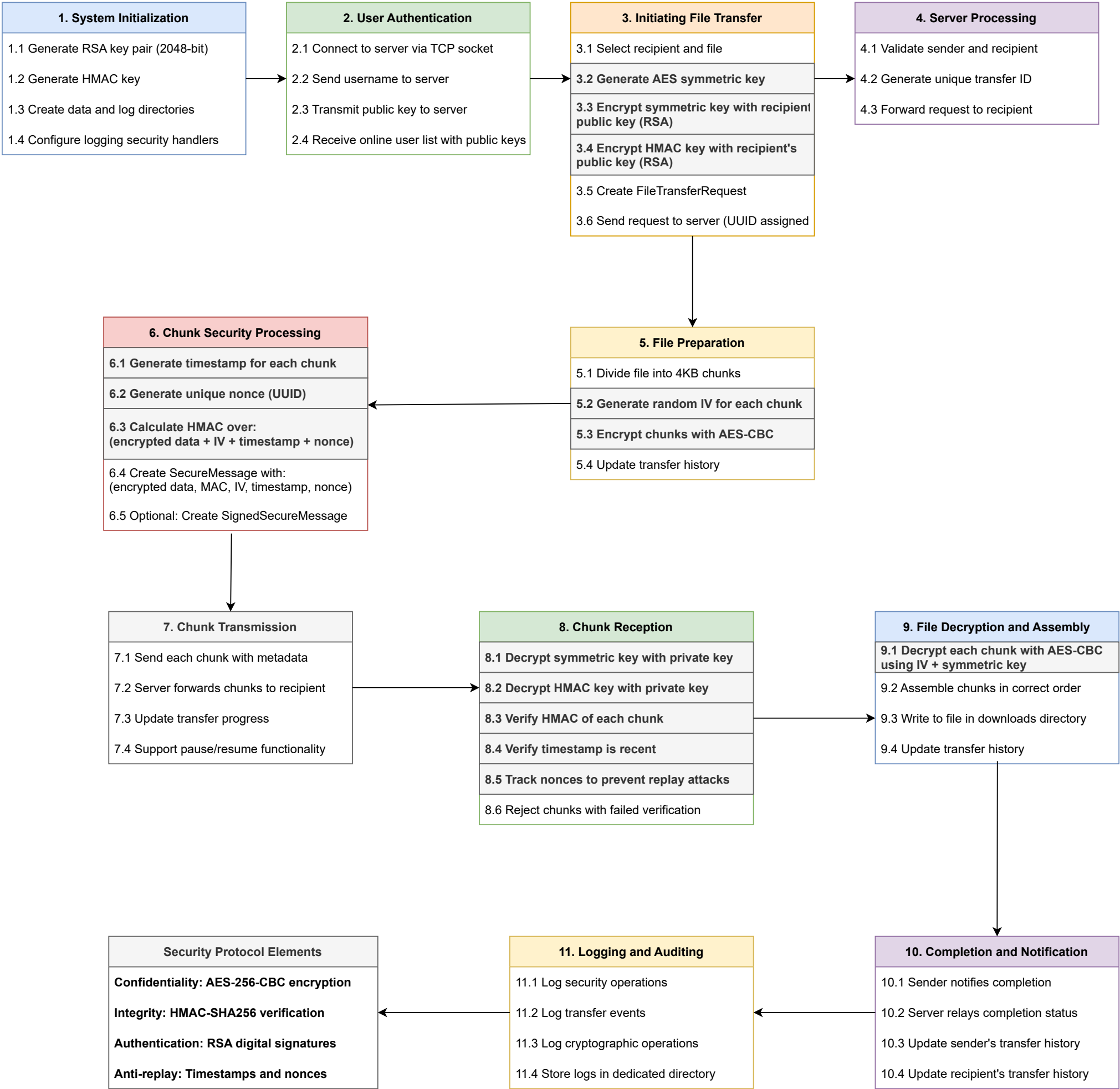
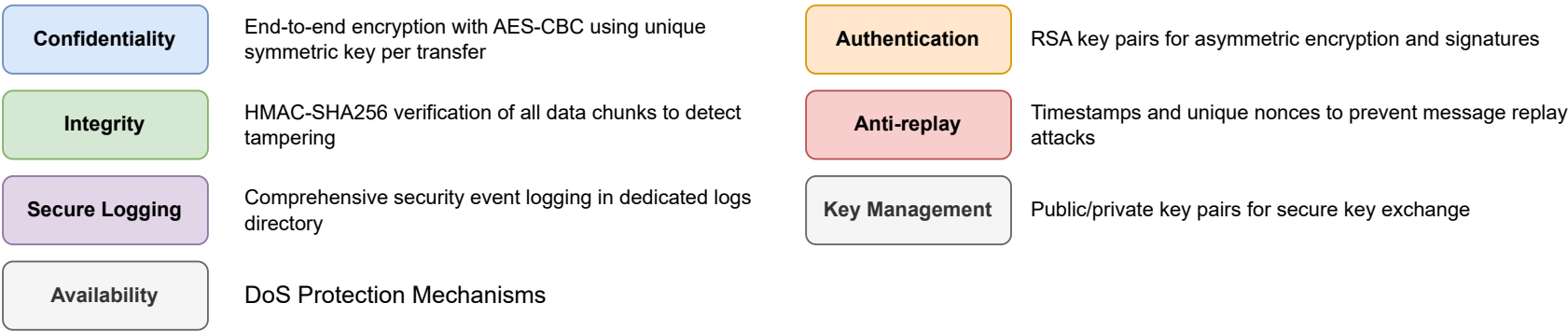


Secure File Transfer Protocol - Security Flow



Key Security Protocol Highlights



DoS Protection Mechanisms

DoS Protection Implementation Flow

<div>Connection Limiting</div> <div>D1.1 Check connection count per IP</div> <div>D1.2 Enforce MAX_CONNECTIONS_PER_IP</div> <div>D1.3 Log excessive connection attempts</div> <div>D1.4 Implement connection timeouts</div>	<div>Request Rate Limiting</div> <div>D2.1 Track requests per minute per IP</div> <div>D2.2 Enforce MAX_REQUESTS_PER_MINUTE (60)</div> <div>D2.3 Exempt file chunk transfers from limits</div> <div>D2.4 Return "Rate limit exceeded" error</div>	<div>IP Blacklisting System</div> <div>D3.1 Record suspicious IP activity</div> <div>D3.2 Blacklist IPs after threshold violatio</div> <div>D3.3 Apply temporary blacklist with expiratic</div> <div>D3.4 Auto-cleanup expired blacklist entries</div>
<div>Login Attempt Limiting</div> <div>D4.1 Track login attempts per hour per IP</div> <div>D4.2 Enforce MAX_LOGIN_ATTEMPTS_PER_HOUR</div> <div>D4.3 Auto-blacklist after exceeding threshold</div>	<div>Bandwidth Control</div> <div>D5.1 Track bandwidth usage per connection</div> <div>D5.2 Enforce BANDWIDTH_LIMIT_BYTES_PER_SEC</div> <div>D5.3 Sliding window for bandwidth calculation</div>	<div>Active DoS Monitoring</div> <div>D6.1 Regular security metric evaluation</div> <div>D6.2 Threshold-based threat level detect</div> <div>D6.3 Automated defense activation</div> <div>D6.4 Administrative alerting</div>

