B.11 Inhaltsverzeichnis Kryptokonzept (Muster)

1. Definitionen

2. Gefährdungslage zur Motivation
- Abhängigkeit der Institution vom Datenbestand
- Typische Gefährdungen
- Institutionsrelevante Schadensursachen
- Schadensfälle im eigenen Haus

3. Festlegung einer organisationsinternen Sicherheitspolitik
- Festlegung von Verantwortlichkeiten
- Zielsetzung, Sicherheitsniveau

4. Einflussfaktoren
- Identifikation der zu schützenden Daten
- Vertraulichkeitsbedarf der Daten
- Integritätsbedarf der Daten
- Verfügbarkeitsanforderungen an die Daten
- Anforderungen an die Performance
- Schlüsselverteilung
- Datenvolumen
- Art der Daten (lokal / verteilt (LAN/WAN))
- Art der Anwendungen, bei denen kryptographische Verfahren zum Einsatz kommen sollen
- Häufigkeit des Einsatzes des kryptographischen Verfahrens
- Anforderungen an die kryptographische Stärke der Algorithmen bzw. Verfahren
- Wiederherstellbarkeit der gesicherten Daten
- Personalaufwand
- Erforderliche Funktionalität
- Kosten einschließlich Folgekosten (Wartung, Administration, Updates, ...)
- Kenntnisse und datenverarbeitungsspezifische Qualifikationen der IT-Benutzer/innen

5. Festlegung des Einsatzes
- Art der kryptographischen Verfahren
- Einsatzbedingungen an die kryptographischen Produkte
- Häufigkeit und Zeitpunkt des Einsatzes
- Benennung der Verantwortlichen
- Festlegung der organisatorischen Regelungen
- Durchführung der personellen Maßnahmen (Schulung, Vertretungsregelungen, Verpflichtungen, Rollenzuteilung)
- Dokumentation der Einsatzbedingungen / Konfiguration
- Interoperabilität, Standardkonformität, Investitionsschutz

6. Schlüsselmanagement