Evangelische Landeskirche
In Württemberg

IT-Konzept

der
Evangelischen Landeskirche
in Württemberg

Datenschutz
und Datensicherheit

Stuttgart, im Juni 2007

Herausgegeben von

Referat Informationstechnologie
Evangelischer Oberkirchenrat
Gänsheidestraße 4
70184 Stuttgart

XI Datenschutz und Datensicherheit

Derzeit werden im Bereich des Oberkirchenrats die eingesetzten Verfahren nach dem IT-Grundschutzhandbuch des Bundesamtes für die Sicherheit in der Informationstechnik dokumentiert und die organisatorischen, infrastrukturellen und technischen IT-Sicherheitsmaßnahmen dargestellt und soweit noch nicht vorhanden, dann auch umgesetzt.

Die Erstellung und Anwendung eines IT-Sicherheitskonzepts wird allen kirchlichen Körperschaften, in denen Informationstechnologie zum Einsatz kommt, dringend empfohlen.

1. Datenschutz und -Sicherheit –Grundsatz–

Anwendungen sind nach dem Prinzip der Datensparsamkeit so zu realisieren, dass sie möglichst wenig personenbezogene Daten verarbeiten. Spezifische Datenschutz- und Sicherheitskonzepte sind, sofern noch notwendig, in Übereinstimmung mit Recht, Organisation und Technik und auf der Grundlage der Rahmenkonzepte systematisch und vollständig zu entwickeln und umzusetzen.

2. Rahmenkonzepte

Die wesentlichen Regelungen des IT-Konzepts zu Datenschutz und Datensicherheit (aufgrund der einschlägigen Vorschriften) bei Client-Server-Systemen sind:

- Freeware/Shareware aus dem Internet darf grundsätzlich dienstlich nicht eingesetzt werden. In Ausnahmefällen kann der Einsatz solcher Software aber durchaus sinnvoll sein; die dafür in Frage kommenden Programme sind in Anlage 2 -Software- zu diesem Konzept genannt.
- Der Einsatz von unzulässig beschafften oder für den Dienstgebrauch nicht freigegebenen dezentralen Systemen (Hard- und Software) ist verboten.
- Dezentrale Systeme werden nach dem Stand von Organisation und Technik (nicht nach dem Stand der Wissenschaft oder der allerneuesten Technik) gesichert.
- Jedes Computersystem wird so gesichert, dass einfache bis schutzwürdige Daten damit verarbeitet werden können. Nur für die regelmäßige Verarbeitung von als vertraulich klassifizierten Daten sind besondere Maßnahmen notwendig.
- Die Sicherheit dezentraler Systeme wird von den jeweiligen Betreibern vor der Inbetriebnahme und danach in regelmäßigen Abständen nach dem IT-Grundschutzhandbuch des BSI in einem angemessenen Detaillierungsgrad analysiert und dokumentiert. Das Ergebnis einer solchen Analyse ist letztendlich maßgeblich und bildet den Ausgangspunkt des Sicherheitskonzepts, das jede Dienststelle für ihre Client-Server-Systeme erstellt.
- Die Sicherheit eines dezentralen Systems darf nicht die Sicherheit eines anderen, mit ihm vernetzten Systems beeinflussen.
- Ein Client-Server-System wird mit dem LAN und den dort installierten Routern als Einheit gesehen und auch so gesichert.
- Im Regelbetrieb eingesetzte Sicherheitstechnik muss bewährt und erprobt sein.
- Eine Dienststelle kann ihre dezentralen Systeme im Auftrag (z. B. Outsourcing) betreiben lassen. Für Datenschutz und Datensicherheit ist in jedem Fall die Daten verarbeitende Stelle i. S. des DSG-EKD zuständig.

Verschlüsselungstechnik wird insbesondere eingesetzt, wo

- die Sensitivität oder Vertraulichkeit der Daten dies erfordert (z. B. Verschlüsselung sensibler Dokumente auf einem PC, der Zugang zum Internet hat) oder
- Schwachstellen anders nicht beseitigt werden können oder
- schutzwürdige personenbezogene Daten über Netze unbekannter Betreiber (betrifft insb. das Internet) übertragen werden oder voraussichtlich den Geltungsbereich der deutschen Gesetze verlassen oder
- durch den Einsatz der Verschlüsselungstechnik Kosten bei klassischen Sicherheitsmaßnahmen reduziert werden können (z. B. Austausch von vertraulichen Vertragsunterlagen über das Internet anstatt in Papierform).
- Die Verschlüsselungstechnik muss zu den sonstigen Sicherheitsmaßnahmen passen, dem Stand der Technik entsprechen und teure Insellösungen vermeiden. Deshalb erfolgt der Einsatz von Verschlüsselungstechnik nur im Einvernehmen mit der Stabsstelle, das so früh wie möglich herzustellen ist.
- Amerikanische Verschlüsselungstechnik kann eingesetzt werden, sofern die seit 17.07.2000 exportierbaren hoch sicheren US-Versionen eingesetzt werden.

Die technischen und organisatorischen Maßnahmen müssen auf der Basis eines vollständigen Sicherheitskonzepts systematisch eingesetzt werden, um einen insgesamt hohen Sicherheitsstandard zu erreichen.

Im Hinblick auf die organisatorischen Maßnahmen wird unterschieden zwischen Systemen, die keine personenbezogenen Daten oder nicht schutzbedürftige personenbezogene Daten verarbeiten und solchen, die schutzwürdige personenbezogene Daten verarbeiten.

Vor einer produktiven Nutzung eines dezentralen Systems wird eine Sicherheitsprüfung durchgeführt und dokumentiert. Dezentrale Systeme und jedes der dort eingesetzten IT-Verfahren zur Verarbeitung personenbezogener Daten werden nach dem vorgesehenen Freigabeverfahren durch die Landeskirche freigegeben.

3. Virenschutz und Firewalltechnik

Standard	Beschreibung/Definition	Einsatz/Begründung
Virenschutz Landes-Standard	Das durchgängige, mehrstufiges Virenschutzkonzept im IT-Konzept besteht u. a. aus: • Virenscanner beim Mailverkehr (Gateway und Postfachspeicher) HTTP/HTTPS/FTP- • permanent aktiver Virenschutz auf Server (in Echtzeit) • permanent aktiver Virenschutz auf Clients(durch Anwender nicht abschaltbar) • periodisches und automatisiertes, beim Bekannt werden neuer Viren jedoch unverzügliches Update der neuesten Anti-Viren-Pattern durch Herunterladen über das Internet und Verteilung im Netzwerk • evtl. zusätzliche Sicherheit durch den Einsatz von Anti-Viren-Produkten verschiedener Herstellern auf den einzelnen Plattformen (Exchange-Server, Clients) prüfen und ggf. realisieren.	Einsatz: Mehrstufiger Einsatz führt zu höherer Betriebssicherheit und erhöht die Datensicherheit durch Vermeidung von Datenverlusten durch bösartige Programme. Begründung: • Kosteneinsparungen durch Verhinderung von aufwendigen Wiederherstellungsmaßnahmen bei Datenverlusten/Datenzerstörung. • Bestandteil der einheitlichen IT-Infrastruktur.
Schutz gegen Makroviren	Office • Sicherheitseinstellungen in Office • Digital signierte Makros • Trust-Center für digital signierte Makros beim OKR	Einsatz: Die Kirchliche Verwaltung setzt künftig grundsätzlich nur noch digital signierte Makros ein. Für Makro-Signaturen durch den OKR gilt die in der EDV-Kommission abgestimmte Policy.

Standard	Beschreibung/Definition	Einsatz/Begründung
Standardisierter Firewall Internet-Standard	Die Aufgabe von Firewalls ist es, einen möglichst ungestörten Zugriff der Intranets der Ressorts auf das öffentliche Netzwerk zu gewährleisten, andererseits den unberechtigten Zugriff auf das eigene Netz zu verhindern. Ein Firewall stellt daher den einzigen Zugang des eigenen Netzes zum öffentlichen Netzwerk dar. Die Firewall beim OKR besteht in der Regel aus Hard- und Software-Komponenten, die entsprechend der Anforderung des IT-Konzepts ganz bestimmte Dienste freigeben. Durch die Konzentration des Zugangs auf eine einzelne Komponente werden das Sicherheits-Management und die Überwachungs- und Kontrollfunktionen wesentlich vereinfacht. Bei den Zugriffskontrollsystemen von Firewalls unterscheidet man dem Verfahren nach die Datenpaket-Filterung, das Circuit-Relay und den Application-Gateway. Alle drei Funktionalitäten setzen auf unterschiedlichen Schichten auf und verbinden das Internet mit dem Landeskirchennetz.	Einsatz: Als Protokolle, die Firewalls zu externen Netzen ohne weiteres Sicherheitskonzept mit Standard-Sicherheitsfunktionen passieren lassen, sind zugelassen: • HTTPS • SMTP • LDAP • DNS. Dies sind auch die Protokolle des standardisierten Firewalls. Die Nutzer von Firewalls müssen Restrisiken einplanen.

4. Erstellung von Sicherheitskonzepten

Standard	Beschreibung/Definition	Einsatz/Begründung
Allgemein	Fundstelle: IT-Grundschutzhandbuch des BSI, Ausgabe 2004 Bei einem Schutzbedarf "niedrig bis mittel" reichen i. d. R. die Standardsicherheitsmaßnahmen des IT-Grundschutzhandbuchs aus. Bei einem Schutzbedarf "hoch bis sehr hoch" kann es sinnvoll sein zu prüfen, ob die Standardsicherheitsmaßnahmen durch höherwertige, meist jedoch auch kostspieligere, IT-Sicherheitsmaßnahmen ergänzt oder ersetzt werden müssen. Welche zusätzlichen Maßnahmen geeignet sind, kann nach Durchführung des Basis- Sicherheitschecks nach IT-Grundschutz mittels einer ergänzenden Sicherheitsanalyse (z. B. Risikoanalyse) festgestellt werden.	Einsatz: IT-Systeme der Landeskirche im Rahmen des IT-Konzepts haben in der Regel differenzierten Schutzbedarf. Deshalb ist das IT-Grundschutzhandbuch anzuwenden.
Schutzbedarfsfeststellung	Ausgehend von den 3 Grundbedrohungen 1. Verlust der Unversehrtheit 2. Verlust der Vertraulichkeit 3. Verlust der Verfügbarkeit wird für das untersuchte IT-System ermittelt, welche Schäden bzw. Folgen durch Sicherheitsverletzungen entstehen würden. Beispiele: • Verstöße gegen Gesetze, Vorschriften, Verträge • Beeinträchtigung des informationellen Selbstbestimmungsrechts • Beeinträchtigung der persönlichen Unversehrtheit • Beeinträchtigung der Aufgabenerfüllung • Finanzielle Auswirkungen. Daraus ergibt sich der konkrete Schutzbedarf.	Einsatz: IT-Anwendungen der Landeskirche im Rahmen des IT-Konzepts haben in der Regel differenzierten Schutzbedarf. Deshalb ist das IT-Grundschutzhandbuch anzuwenden.
Risikoanalyse	Die Risikoanalyse setzt immer auf einer Schutzbedarfsfeststellung auf (siehe IT-Grundschutzhandbuch). Wird nach Durchführung des Basis-Sicherheitschecks nach IT-Grundschutz der Bedarf nach einer erweiterte Sicherheitsanalyse erkannt, empfiehlt es sich, zunächst eine Bedrohungsanalyse durchzuführen, bei der die bedrohten Objekte des IT-Systems und alle vorstellbaren Bedrohungen (Schwachstellenanalyse) in angemessenem Umfang ermittelt werden.	Einsatz: IT-Anwendungen der Landeskirche im Rahmen des IT-Konzepts haben in der Regel differenzierten Schutzbedarf. Deshalb ist das IT-Grundschutzhandbuch anzuwenden.

Standard	Beschreibung/Definition	Einsatz/Begründung
	Die Objektbildung kann z. B. nach folgenden Gruppen gegliedert werden: 1. Infrastruktur 2. Hardware 3. Software 4. Datenträger 5. Anwendungsdaten 6. Kommunikation 7. Personen Wobei zweckmäßigerweise alle wesentlichen Prozesse und Datenströme zerlegt und die Teile auf Manipulationsmöglichkeiten hin untersucht und bewertet werden. Bei der anschließenden Risikobetrachtung werden die Schadenswerte/ Häufigkeiten der Bedrohungen für die Objekte bewertet und daraus das differenzierte Sicherheitsrisiko R (R = p*S; p= Wahrscheinlichkeit für einen Schaden, S= mittlerer Schaden) ermittelt.	
Sicherheitskonzept	Hier werden die Maßnahmen gegen die Bedrohungen ausgewählt und ihre Wirkungen beurteilt. Dabei ist zu entscheiden, welche Maßnahmen angemessen sind (Kosten-Nutzen-Betrachtung) und welches Restrisiko tragbar ist.	

5. Internet-Anschluss

Standard	Beschreibung/Definition	Einsatz/Begründung
Landeskirchlicher Standard	Netze einer Kirchlichen Verwaltung dürfen nur auf der Grundlage eines detaillierten Sicherheitskonzepts an das Internet angeschlossen werden. Benutzer des OKR-Netzes können über ein logisches Intranet mittels zentralen Internet-Zugangs des OKR, der durch ein Firewallsystem und einen zentralen Virenscanner geschützt ist, an das Internet angeschlossen werden. Die Dienststellen, die einen Internet-Zugang in ihrem LAN bereitstellen, müssen sicherstellen, dass dadurch keine Störungen, Eindringversuche oder sonstige Risiken in irgendeiner Benutzergruppe des Netzes entstehen. Bei Internet-Anschlüssen ist zudem sicherzustellen, dass durch klare Zuständigkeitsregelungen eine laufende tatsächliche Kontrolle und Aktualisierung der Technik sichergestellt ist. Datenbestände, die dem Risiko des Internetzugangs nicht ausgesetzt werden dürfen, sind durch physische Trennung oder Verschlüsselung (z. B. durch PGP) zu schützen.	Einsatz: IT-Systeme müssen so betrieben werden, dass sie andere Systeme nicht stören oder an sie Störungen weiterleiten. Durch den Betrieb eines zentralen und leistungsfähigen Internet-Anschlusses über einen mit modernen Tools professionell administrierten Firewall werden Kosten und Sicherheitsrisiken minimiert.

6. Sicherheit bei Telearbeit und bei Arbeit außerhalb der Dienststelle

Die Standards des IT-Konzepts berücksichtigen die personalrechtlichen Fragen, die Organisation der Telearbeit und Definitionen zur Telearbeit nicht, sondern beschränken sich auf Empfehlungen zu Sicherheitsmaßnahmen, die bei der Nutzung privater oder dienstlicher Geräte für dienstliche Zwecke notwendig werden. Deshalb werden die Bestimmungen in der Arbeitsrechtlichen Regelung zur Telearbeit –Dienstzimmer im Privatbereich– Beschluss der Arbeitsrechtlichen Kommission vom 8.Dezember 2006 (Abl. 62 S. 328) durch die hier genannten Sicherheitsmaßnahmen ergänzt.

Aus Sicht des IT-Konzepts kann den Bediensteten grundsätzlich erlaubt werden, mit privaten Geräten sicherheitsmäßig unbedenkliche Verarbeitungsvorgänge durchzuführen. Solche Vorgänge sind z. B. dienstliche Anrufe über private Handys, dienstlich relevante SMS über private Handys, Erstellung von Vorträgen und Vortragsfolien mit privatem PC, sofern keine sensiblen Informationen übertragen werden und durch den Datenaustausch mit dem privaten Gerät keine Gefährdung dienstlicher Informationstechnologie entsteht.

CITRIX-Portal (siehe Kapitel III Netz- und Kommunikationsstrukturen, Punkt 9. Portal, Seite 20).

Darüber hinaus gilt, dass der Nutzer privater Informationstechnologie in der Lage sein muss, die dabei anfallenden technischen Vorgänge bezüglich des Risikos zu bewerten.

Standard	Beschreibung/Definition	Einsatz/Begründung
Handys, Personal Digital Assistants, Subnotebooks und Smartphones sowie Notebooks	Sicherheitsfragen bestehen bei der genannten Gerätegruppe je nach Ausstattung und Leistungsfähigkeit der Geräte insb. bezüglich • der Vertraulichkeit bei der Verarbeitung (z. B. Vertraulichkeit von Adressverzeichnissen, Personenlisten, Vermerken z. B. im Zusammenhang mit einer Vergabe, Arbeit an öffentlichen Plätzen wie z. B. bei einer Dienstreise) • der Abschottung gegenüber Dritten (z. B. beim Vergessen eines Geräts im Zug, beim Hinterlassen eines Geräts im Hotelzimmer während der Einnahme von Mahlzeiten) • der Aktualisierung von Verzeichnissen und Dokumentenablagen (z. B. Vermeiden von falschen Verarbeitungsvorgängen) • Verhindern einer Benutzung durch Dritte (z. B. sollen Diebe eine SIM-Card oder ein Notebook nicht oder zumindest nicht ohne weiteres nutzen können) • Verhindern von zufälligen Fehlern (z. B. Bedienungsfehler).	Dienstlich bereitgestellte Geräte sind immer durch ein Passwort zu sichern. Auf einem privaten Gerät dürfen keine dienstlichen Daten verarbeitet werden. Wenn regelmäßig vertrauliche oder sensible Informationen gespeichert oder sonst verarbeitet werden und das Gerät von Dritten unbefugt benutzt werden könnte, müssen die schützenswerten Daten nach dem Stand der kommerziellen Technik verschlüsselt werden.
Telearbeitsplätze ohne direkten Zugriff auf das dienstliche Bürokommunikationssystem	Soweit kein zwingender Bedarf vorhanden ist, werden Telearbeitsplätze aus Sicherheits- und Kostengründen nur über E-Mail-Verbindungen mit dienstlichen Bürokommunikationssystemen vernetzt. Solche Telearbeitsplätze haben i. d. R außerdem Zugang zum Internet. Telearbeiter müssen beim Einsatz der Telearbeitstechnik die Wirtschaftlichkeit ständig berücksichtigen.	Wenn vertrauliche oder sensible Informationen über das Internet übertragen werden, sind die Daten bei der Übertragung zu verschlüsseln. Der Telearbeiter muss, wenn er andere Internet-Dienste als E-Mail nutzt, die Risiken kennen und sicherstellen, dass durch seine Internet-Nutzung keine Risiken für die dienstliche Informationstechnologie entstehen. Eine Authentifikation über Passwort ist vorzusehen. Die allgemein üblichen Passwort-Regelungen (vgl. z. B. Empfehlungen des Datenschutzbeauftragten im Internet) sind umzusetzen. Der Telearbeiter muss den Datenbestand auf seinem PC so verwalten, dass er alle Anforderungen der Datenschutzvorschriften (insb. Richtigkeit, Auskunft über die gespeicherten

Standard	Beschreibung/Definition	Einsatz/Begründung
		Daten und die benutzten Verfahren, Übermittlungskontrolle, Löschung z. B. bei veralteten Daten oder bei Fehldrucken) erfüllt.
Telearbeitsplätze mit direktem Zugriff auf das dienstliche Bürokommunikationssystem	Bei diesen Telearbeitsplätzen sind neben den o.g. Sicherheitsmaßnahmen noch Maßnahmen zum sicheren Zugang zu dem dienstlichen Bürokommunikationssystem zu ergreifen.	Der Zugang zum dienstlichen Bürokommunikationssystem muss zusätzlich zu den o. g. noch folgende Anforderungen erfüllen: • Sichere Authentifikation des Telearbeiters • Aktivierung der Abschottungsregeln im dienstlichen Bürokommunikationssystem beim Telearbeitszugang, die beim Zugang im Büro gelten • Verschlüsselung des Datenverkehrs, falls ausländische Netze genutzt werden könnten • Automatische Erkennung von Kommunikationsstörungen mit automatischem Abmelden des Telearbeiters. Einsatz: Im OKR wird das CITRIX-Portal (s.III.9.1) als Zugang angeboten.

7. Zugriffssicherung/Berechtigungsprüfung

Standard	Beschreibung/Definition	Einsatz/Begründung
Basis-Authentifizierung	Dieses Standard-Verfahren zur Absicherung von Benutzerzugriffen auf Serveranwendungen beruht auf der Prüfung von Benutzername und Passwort. In Intranets mit heterogenen Client-Server-Umgebungen und im Internet werden diese Login-Parameter unverschlüsselt im Netz übertragen. Daraus ergibt sich ein erhöhtes Sicherheitsrisiko. In homogenen Client-Server-Umgebungen wie z. B. Windows erfolgt diese Übertragung teilweise verschlüsselt.	Einsatz: Regelmäßig bei Grundverfahren der einheitlichen IT-Infrastruktur und bei Netzwerk- Anwendungen innerhalb des OKR-Intranets. Dieses Verfahren ist als Sicherheitsmaßnahme im Internet grundsätzlich nicht geeignet.
Höherwertige Authentifizierung Internet-Standard	Dieses Verfahren unterstützt sowohl die Authentifizierung als auch die gesicherte Datenübertragung. Für eine sichere und vertrauliche Kommunikation über öffentliche Netze sind folgende Lösungen einzusetzen: • Kommunikationsebene: Basis SSL V.3 bzw. TLS V1.0 ggf. mit Client-Authentifizierung ; SSL/TLS nutzt die Public Key Kryptografie zur Authentifizierung und die Secret Key Kryptografie zur Verschlüsselung der auszutauschenden Nachrichten; die Schlüsselzertifikate (Client und Server) müssen von Zertifizierungsinstanzen stammen, die von Clients und Server anerkannt werden. • Anwendungsebene: Einmalpasswörter in Verbindung mit Authentifizierungsservern ermöglichen ein sicheres Login. Einmalpasswörter werden für jeden Loginvorgang auf speziell programmierten Token neu erzeugt. Für den sicheren Datenaustausch sorgen dann Verschlüsselungsprogramme.	Einsatz: Insbesondere wenn Zugriffe über fremde Netze erfolgen oder wenn ein Firewall einfacher gestaltet werden soll, ist eine Sicherung über die SSL-Mechanismen geboten.

8. Kryptografische Verfahren

8.1. Kryptografische Standards

Schlüssellänge und Verfahren sind bei den kryptografischen Standards zusammenhängend zu betrachten.

Standard	Beschreibung/Definition	Einsatz/Begründung
Symmetrische Verfahren		Einsatz: Typisches Anwendungsgebiet für symmetrische Algorithmen ist die vertrauliche Speicherung von Daten auf lokalen Laufwerken (z. B. Festplatten, Disketten) oder auf einem Server
DES ANSI-Standard	Fundstelle: ANSI (American National Standards Institute) X3.92-1981 (Data Encryption Standard) Der DES-Algorithmus (für Anwendungs- und Kommunikationsebene) ist ein Blockchiffrierer, der unter Verwendung eines 64 Bit Schlüssels (56 Bits signifikant, 8 Paritätsbits) 64 Bits Klartext in 64 Bits Schlüsseltext transformiert	Einsatz: Vom Einsatz wird abgeraten Begründung: DES ist zwar weit verbreitet, allerdings auf Grund der geringen Schlüsselgröße von 56 Bits umstritten.
3DES NIST-Standard	Fundstelle: NIST -Standard (National Institute of Standards and Technology) Triple-DES (3DES) erhöht die Sicherheit des normalen DES-Verfahrens, indem die Daten mit doppelter (112 Bit) oder dreifacher (168 Bit) Schlüssellänge verschlüsselt werden.	Einsatz: Stärkere Verschlüsselung, deshalb Einsatz bei höherem Sicherheitsbedarf sinnvoll.
IDEA	IDEA (International Data Encryption Standard) ist ähnlich wie DES ein symmetrischer IDEA (International Data Encryption Standard) ist ähnlich wie DES ein symmetrischer Verschlüsselungs-Algorithmus. IDEA verwendet eine Schlüssellänge von 128 Bit.	Wie 3DES
AES	AES (Advanced Encryption Standard, auch Rijndael genannt) soll den DES Standard ablösen. Das National Institute of Standards and Technology (NIST) hat AES am 26.11.2001 zum Standard erklärt. Erste Produkte sind verfügbar. Geforderte Schlüssellängen im AES-Standard sind 128, 192 und 256 Bit.	Einsatz: Da inzwischen in der Presse erste Berichte zu erfolgreichen Angriffen auf AES erschienen sind, sollten vor einem Einsatz noch weitere Erfahrungen abgewartet werden.
Asymmetrische Verfahren		
RSA	Fundstelle: R. Rivest, A. Shamir, L. Adleman: *A method for obtaining digital signatures and public key cryptosystems, Communications of the ACM*, Jahrgang 21, Nr. 2 (1978) RSA basiert auf dem Schlüsselaustausch-Algorithmus von Diffie-Hellmann (1976), der die Grundlage für die Public Key Kryptografie darstellt. Während symmetrische Verfahren darauf beruhen, dass Daten und Informationen mit demselben Schlüssel ver- und entschlüsselt werden, wird beim asymmetrischen Verfahren ein Schlüsselpaar, bestehend aus dem geheimen (private Key) und dem öffentlichen Schlüssel (public Key) verwendet. Daten, die mit einem öffentlichen Schlüssel verschlüsselt werden, können nur mit dem zugehörigen geheimen Schlüssel entschlüsselt werden und umgekehrt. Die Berechnung des geheimen Schlüssels zu einem vorgegebenen öffentlichen Schlüssel beruht beim RSA-Verfahren auf der Faktorisierung großer Zahlen, d.h. der Zerlegung in ihre Primfaktoren. Das RSA-Verfahren ist auch die Grundlage für die elektronische Signatur, bei der die zu signierenden Daten zunächst mit einem geeigneten Zufallsverfahren komprimiert werden	Einsatz: Regelmäßig im Zusammenhang mit allen Verfahren zur • Ende-zu-Ende- Verschlüsselung der elektronischen Post • elektronischen Signatur Begründung: RSA ist heute Standard für die asymmetrische Verschlüsselung mit und ohne Chipkarten bis Schlüssellangen von ca. 2048 Bits. Für größere Schlüssellängen wird das Verfahren bei der elektronischen Signatur und Entschlüsselung sehr aufwendig. Deshalb ist hier die Elliptic Curve Cryptography (ECC) als Alternative zu RSA sehr stark im Kommen.

Standard	Beschreibung/Definition	Einsatz/Begründung
	und dieses Komprimat dann mit dem geheimen Schlüssel des Signierenden verschlüsselt werden. In Verbindung mit einer durch ein Zertifikat erfolgten Personalisierung des zugehörigen öffentlichen Schlüssels kann der Nachweis der Unversehrtheit der signierten Daten und der Authentizität des Signierenden erbracht werden.	
DSS	Fundstelle: NIST FIPS Publication 186: *Digital Signature Standard*, Mai 1994: 1984 hat El'gamal einen zu RSA alternativen Signaturalgorithmus vorgeschlagen. Eine Variante dieses El'gamal-Verfahrens ist der 1991 von NIST publizierte Standard DSS, der den Digital Signature Algorithmus (DSA) spezifiziert. Neue Varianten des DSA basieren auf Punktegruppen elliptischer Kurven.	Einsatz: Ggf. künftig als Alternative zu RSA für die elektronische Signatur zulässig Begründung: Veröffentlichung der RegTP über "Geeignete Kryptoalgorithmen", BundesAnz. Nr. 158 S. 18 562 vom 24.08.2001
Hybrid Verfahren	Kombination aus symmetrischen (in der Regel DES, 3DES) und asymmetrischen Verfahren (RSA) (siehe S/MIME und PGP, Nr. 9.6.2) Hierbei wird die Nachricht vom Absender zunächst mit einem zufällig generierten Schlüssel symmetrisch verschlüsselt. Der verwendete Schlüssel wird dann mit dem öffentlichen Schlüssel des Empfängers verschlüsselt und zusammen mit der symmetrisch verschlüsselten Nachricht übermittelt.	Einsatz: Regelmäßig bei allen Verfahren zur Ende-zu-Ende-Verschlüsselung der elektronischen Post.

8.2. Verschlüsselungs-Software

Standard	Beschreibung/Definition	Einsatz/Begründung
Verschlüsselung auf Kommunikationsebene		
SSL V. 3 IETF-Standard	SSL ist eine Entwicklung von Netscape für die sichere Datenkommunikation im WWW, kann jedoch auch für andere Anwendungsprotokolle der TCP/IP-Familie wie Telnet, FTP eingesetzt werden. SSL wird von allen gängigen Internet-Browsern und Server-Produkten unterstützt. Die Spezifikation zu SSL wurde Ende 1995 der Internet Engineering Task Force (IETF) zur Standardisierung vorgelegt. Aktuell ist die Version 3.2 von November 1996, die als Internet-Draft vorliegt.	Einsatz: • für die Sicherung besonderer Inhalte im Netz des OKR. Im Intranetverbund ist die sichere US-Exportversion ausreichend. Das Root-Zertifikat (=Zertifizierungsstellen-Zertifikat) wird bereitgestellt Begründung: Bestandteil der einheitlichen IT-Infrastruktur
TLS V1.0	TLS (Transport Layer Security) ist eine Weiterentwicklung von SSL V.3. Die Protokoll-Version 1.0 wurde 1999 veröffentlicht (RFC 2246). Im Gegensatz zu SSL V.3 ist bei TLS V1.0 die Server-Authentifikation optional. Zur Vermeidung von sog. "man-in-the-middle"-Attacken sollte auf diese Funktion jedoch nicht verzichtet werden.	
IPSec IETF-Standard	Bezeichnung für einen Standard, der Verschlüsselung und Authentifizierung für IP-Netze auf der Vermittlungsschicht regelt IPSec ist sowohl für IPv4 als auch für IPv6 definiert. Die Sicherheit gewährleistet IPSec über einen Authentifizierungsheader und ein Sicherheitseinkapselungspaket (Encapsulating Security Payload -ESP-). Im ESP sind die Nutzdaten des Paketes oder ein komplettes Paket (Tunneling) mit einem symmetrischen Algorithmus (DES, 3DES oder IDES) verschlüsselt. IPSec steht in den heutigen Routern z. B. von CISCO und in Verschlüsselungsboxen z. B. von Utimaco, Biodata zur Verfügung. Innerhalb des FreeS/WAN Projektes gibt es zwei frei verfügbare und durch Exportrestriktionen nicht reglementierte	Einsatz: für die Realisierung von VPN-Lösungen und Tunneling z. B. • zur besonderen Sicherung von Benutzergruppen (z. B. PersonalOffice-Anwender) oder • anstelle von Verschlüsselungslösungen auf Anwendungsebene (z. B. SSL)

Standard	Beschreibung/Definition	Einsatz/Begründung
	Versionen von IPSec für Linux: • Pluto • JI's IPSec von John Ioannidis.	
IKE IETF-Standard	IKE ist ein von der Firma Cisco und der IETF erarbeiteter Protokollrahmen zur Verwaltung von Security Associations in IPSec. ISAKMP (Internet Security Association Key Management Protocol) ist nur ein Rahmenwerk. Eine konkrete Umsetzung ist IKE. Internet Key Exchange (IKE) ist ein Protokoll, das der Verwaltung von Sicherheitskomponenten innerhalb von mit IPSec realisierten VPN dient. IKE wird benötigt, da IPSec die zur Verschlüsselung notwendigen Informationen (Algorithmus, Schlüssel, Gültigkeitsdauer etc.) nicht selbst überträgt, sondern sie aus einer lokalen Sicherheits-Datenbank übernimmt.	Einsatz: Der Einsatz ist in VPN Lösungen zum Austausch von Sicherheitsinformationen erforderlich.
Verschlüsselung auf Anwendungsebene		
Pretty Good Privacy de-facto- Standard	PGP (Pretty Good Privacy), Hybridverfahren aus RSA und IDEA, also eine Kombination aus symmetrischen mit asymmetrischen Verfahren, Public-Key-Verfahren zur Verschlüsselung von Daten PGP ist bei privater Nutzung lizenzkostenfrei; die Nutzung innerhalb der Verwaltung ist jedoch lizenzpflichtig. Für PGP gibt es Plug-Ins sowohl für MS-Outlook als auch für die Mail-Clients der Standard-Web-Browser (MS Outlook-Express, Netscape Messenger). Internet Freeware/ Shareware kann dienstlich nicht eingesetzt werden (vgl. Nr. 9.2). Alternativ kann das vom BSI geförderte GNU Privacy Guard (GnuPG) eingesetzt werden. Allerdings sind GnuPG und PGP derzeit noch nicht vollständig miteinander interoperabel.	Einsatz: soweit zweckmäßig zur • Ende-zu-Ende-Verschlüs-selung der elektronischen Post mit Externen, soweit nicht die gesetzeskonforme elektronische Signatur anzuwenden ist • zum Schutz bei Internetanschlüssen für die Verschlüsselung von lokal zu speichernden Dateien Begründung: Bestandteil der einheitlichen IT-Infrastruktur
MailTrusT (MTT) Nationaler Standard	Standard des Industrieverbands Teletrust e.V., dem alle wichtigen deutschen Hersteller kryptografischer Softwareprodukte für die Ende-zu- Ende-Verschlüsselung angehören MTT setzt auf dem Standard PEM (Privacy Enhanced Mail) auf. Die Version 2 ist weitgehend mit S/MIME V3 identisch und enthält unter anderem: • S/MIME als Austauschformat • Zertifikatsformate nach X.509 V. 3. Der Einsatz mit Mail-Clients von Web- Browsern (z. B. Outlook Express, Netscape Messenger) ist derzeit nur beschränkt möglich. Die Interoperabilität der Produkte auf der Basis von MTT V.2 wurde im Rahmen des Sphinx-Projektes des Bundes untersucht. Um Interoperabilität zwischen unterschiedlichen PKI-Lösungen für die Verschlüsselung (nach MTT V. 2) und die - insbesondere qualifizierte - elektronische Signatur (entsprechend den "Industrial Signature Interoperability Specifications" [ISIS V. 1.2], einem von der Arbeitsgemeinschaft der deutschen Trust Center [AGTC] verabschiedeten Standard) zu erzielen, wurde mit ISIS-MTT ein gemeinsamer Standard entwickelt, der als Version 1.02 seit 19.07.2002 vorliegt. Trust Center bieten inzwischen spezielle Dienstleistungen nach dem ISIS-MTTStandard an (z. B. Zeitstempeldienst der Fa. TTeleSec). Nach den Erfahrungen von Fa. Datev und Fa. secaron unterstützen die auf dem Markt verfügbaren Microsoft-Anwendungen Zertifikate gemäß ISIS-MTT-Spezifikation.	Einsatz: In der landeskirchlichen Verwaltung können im Rahmen dereinheitlichen Bürokommunikation solche Produkte für die Ende-zu-Ende-Verschlüsselung der elektronischen Post eingesetzt werden, die dem Mail-TrusT-Standard V. 2 und ISIS-MTT V 1.02 entsprechen. Danach ist diese Verschlüsselungstechnik in der Regel • nicht einzusetzen beim Versand im LAN • einzusetzen beim Versand über das Internet oder andere unbekannte Netze, sofern im Einzelfall z. B. auf Grund der geringen Schutzbedürftigkeit der versendeten Daten nicht anders entschieden wird. Begründung: Bestandteil der einheitlichen IT-Infrastruktur. ISISMTT wird zu gegebener Zeit aufgenommen.
S/MIME Firmen-Standard	S/MIME basiert ebenfalls auf dem asymmetrischen Schlüsselsystem. Im direkten Vergleich zu PGP ergeben sich folgende Unterschiede: • Im Gegensatz zu PGP bedarf S/MIME immer des Einsatzes von Schlüsselzertfikaten, die von einem Trust Center ausge-	Einsatz: Für die Verschlüsselung von E-Mails ist S/MIME mit einem starken Verschlüsselungsalgorithmus (mindestens 112 Bits Schüssellänge) einzusetzen.

Standard	Beschreibung/Definition	Einsatz/Begründung
	stellt werden. • Weiterhin wird, im Unterschied zu PGP, bei der elektronischen Signatur einer E-Mail immer zwingend das Zertifikat des öffentlichen Schlüssels entsprechend X 509 V. 3 angehängt. • S/MIME garantiert durch die Mail-Struktur nach PKCS # 7, dass eine an mehrere Empfänger (z. B. Verteilerliste) gerichtete verschlüsselte Mail für alle Empfänger dasselbe Format besitzt.	(vgl. Regelungen zu MTT) Begründung: Bestandteil der einheitlichen IT-Infrastruktur

8.3. Standard für Schlüssel-Zertifikate

Standard	Beschreibung/Definition	Einsatz/Begründung
X.509 ITU-Standard	Fundstelle: X.509 ist ursprünglich ein IEEE-Standard, der von der ITU übernommen wurde. Der gebräuchliche Standard für digitale Zertifikate ist der ITU Standard X.509v3. X.509 setzt auf den Namenskonventionen des Verzeichnis-Standards X.500 auf. X.509 definiert den Aufbau und Inhalt (Attribute) für die Zertifikate öffentlicher Schlüssel im Rahmen einer so genannten PKI (Public Key Infrastructure). Ein solches Zertifikat enthält neben dem öffentlichen Schlüssel des Eigentümers Angaben zur Identifikation (Name, ggf. Wohnort, etc.) des Eigentümers und zum Zertifikat selbst (Name der Zertifizierungsstelle, Gültigkeitsdauer des Zertifikats, X.509-Version, Zertifikats-Nummer, etc). Darüber hinaus enthalten Zertifikate i.d.R. eine elektronische Signatur der Zertifizierungsstelle. X.509v3 unterscheidet sich von seinen Vorgänger- Versionen insbesondere dadurch, dass weitere Angaben zum Eigentümer (z. B. Geburtsdatum) oder zum Zertifikat als sog. Extensions hinzugefügt werden können.	Einsatz: Regelmäßig beim Einsatz von asymmetrischen oder hybriden Verschlüsselungsverfahren und bei der elektronischen Signatur. Begründung: Wird eine Institution oder Person zertifiziert, so geschieht dies über die eindeutige Bindung ihres öffentlichen Schlüssels an ihren Namen und weitere Attributinformationen, die das zu zertifizierende Subjekt charakterisieren. Eine Zertifizierungsstelle bestätigt als vertrauenswürdiger Dritter diese Bindung mit elektronischer Signatur. Im Netz des OKR werden die Zertifikate in ein Einheitliches Benutzerverzeichnis eingestellt und können von dort z. B. per LDAP oder http abgerufen werden.

8.4. PKI-Konzept

Um die rechtlichen Anforderungen der Datenschlüsselungsverordnung umzusetzen wurde im Evangelischen Oberkirchenrat eine PKI (Public Key Infrastructure) auf Basis von S/MIME aufgebaut.

Für das Ausstellen und Verteilen der Zertifikate steht im Evangelischen Oberkirchenrat ein Server als Zertifizierungsstelle zur Verfügung. Hier können Zertifikate angefordert und abgeholt werden. Die Zertifikate werden dann auf dem lokalen Rechner gespeichert und stehen damit zur Verfügung. Auch die öffentlichen Schlüssel evtl. E-Mail-Partner können von diesem Server abgeholt werden.

Der Zugang zum Zertifikatsserver erfolgt über die Internet-Adresse: http://pki.elk-wue.de.

Standard	Beschreibung/Definition	Einsatz/Begründung
PKI für die E-Mail-Verschlüsselung	Für eine verschlüsselte Übertragung benötigen Sender und Empfänger ein digitales Zertifikat. Ein digitales Zertifikat ist ein Datensatz, der Informationen über den Namen des Inhabers, dessen öffentlichen Schlüssel, die E-Mail Adresse, eine Seriennummer, eine Gültigkeitsdauer und den Namen der Zertifizierungsstelle enthält. Eine digitale Signatur schützt diesen Datensatz gegen Veränderung. Jeder Teilnehmer an der Verschlüsselung hat einen "Öffentlichen Schlüssel", den jeder bei einer im Netz zugänglichen Stelle abholen kann und der nur zur Verschlüsselung an ihn gerichteter Nachrichten dient. Der Absender verschlüsselt E-Mails mit dem öffentlichen Schlüssel des Empfängers und versendet sie. Nur der Empfänger kann verschlüsselte E-Mail mit seinem privaten Schlüssel entschlüsseln und damit lesen.	Einsatz: Um den dienstlichen E-Mail-Verkehr zwischen Oberkirchenrat, den Kirchlichen Verwaltungsstellen, den Prälaturen, Dekanatämtern und Pfarrämtern in verschlüsselter Form abwickeln zu können, wurde im Evangelischen Oberkirchenrat die Infrastruktur auf der Basis des S/MIME Standards (Secure / Multipurpose Internet Mail Extension, Sicherheits-Erweiterung der E-Mail-Kommunikation) eingerichtet. Für den verschlüsselten Datenverkehr zwischen weiteren Datenstellen kann auch PGP (Pretty Good Privacy, bekannte Verschlüsselungssoftware für Einzelrechner) eingesetzt werden.