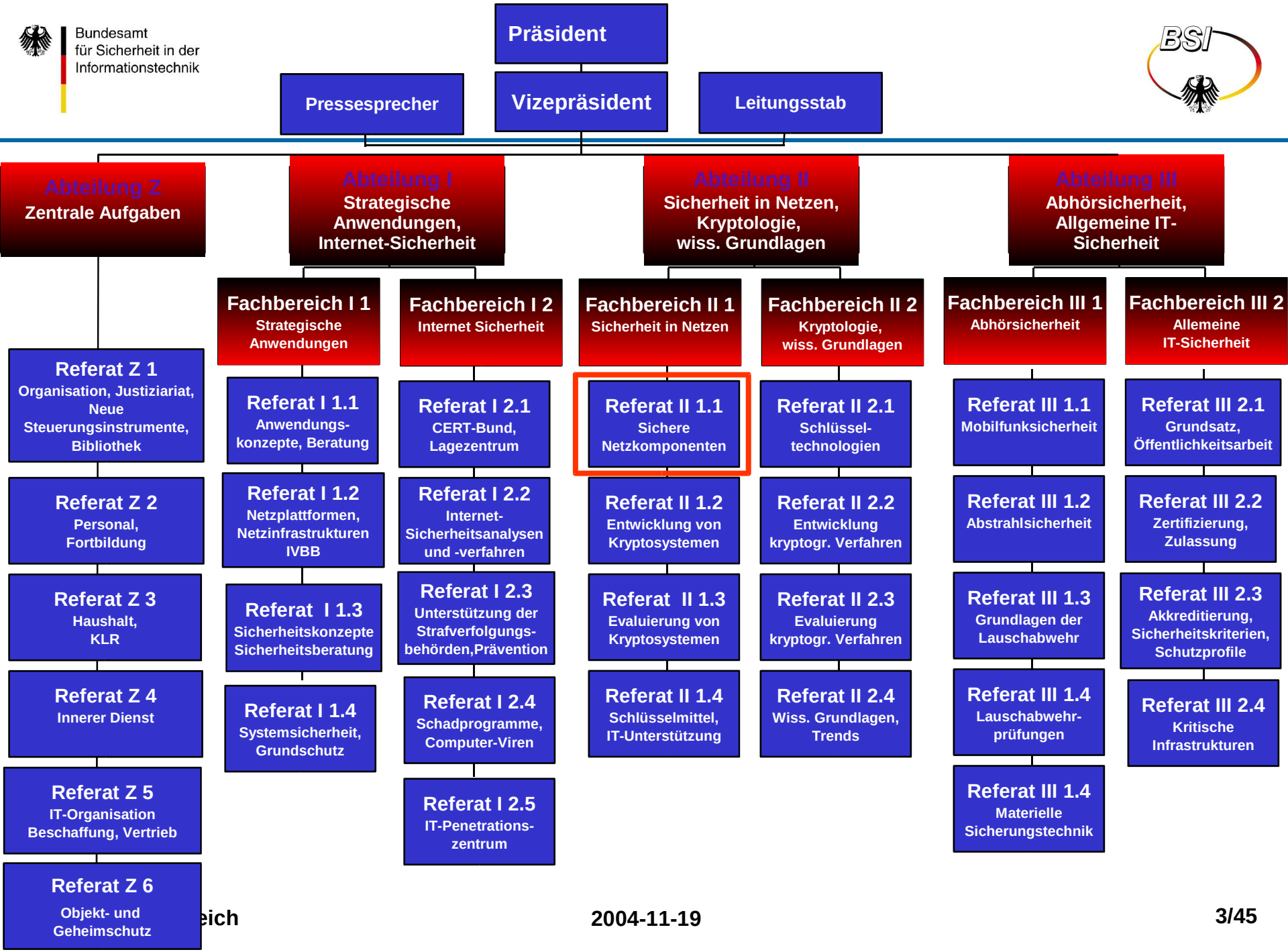
Sichere Inter-Netzwerk Architektur

(I) Überblick

Dr. Thomas Östreich
Bundesamt für Sicherheit in der Informationstechnik
II 1.1 – Sichere Netzkomponenten
thomas.oestreich@bsi.bund.de / +49 (0)1888 9582 466

Das BSI auf einen Blick

- Unabhängige und neutrale Autorität für IT-Sicherheit
- Bundesoberbehörde im Geschäftsbereich des Bundesministerium des Innern (BMI)
- Gegründet 1991 - als Behörde im Vergleich zu sonstigen europäischen Einrichtungen einzigartig
- Personal: ca. 380 Mitarbeiter
- Haushaltsvolumen 2004: 51 Million €

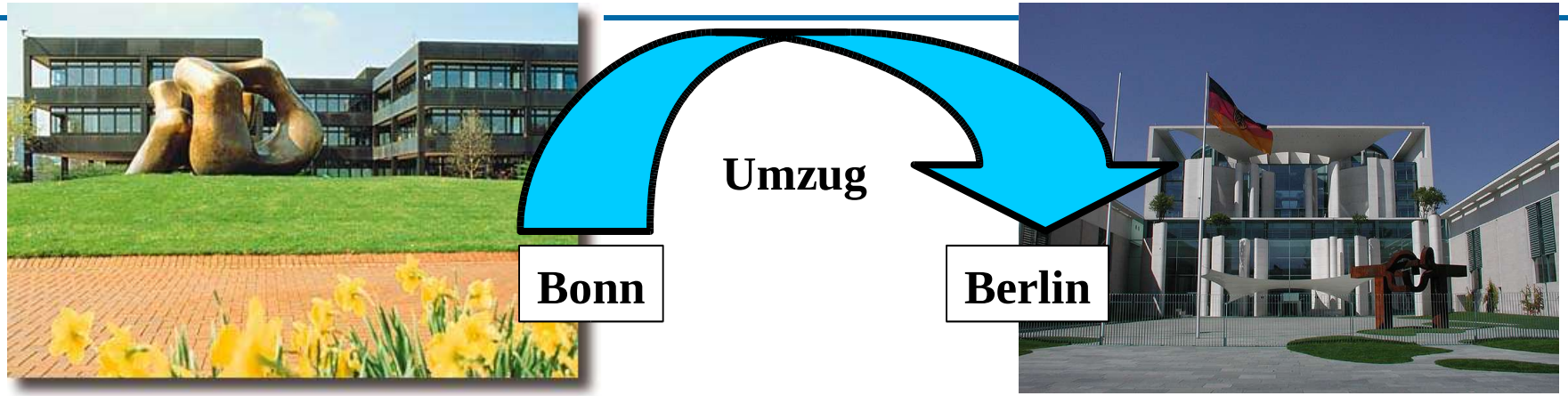

Präsident
Pressesprecher
Vizepräsident
Leitungsstab
Abteilung Z
Zentrale Aufgaben
Abteilung I
Strategische Anwendungen, Internet-Sicherheit
Abteilung II
Sicherheit in Netzen, Kryptologie, wiss. Grundlagen
Abteilung III
Abhörsicherheit, Allgemeine IT-Sicherheit
Referat Z 1
Organisation, Justiziariat, Neue Steuerungsinstrumente, Bibliothek
Referat Z 2
Personal, Fortbildung
Referat Z 3
Haushalt, KLR
Referat Z 4
Innerer Dienst
Referat Z 5
IT-Organisation Beschaffung, Vertrieb
Referat Z 6
Objekt- und Geheimschutz
Fachbereich I 1
Strategische Anwendungen
Fachbereich I 2
Internet Sicherheit
Referat I 1.1
Anwendungs-konzepte, Beratung
Referat I 1.2
Netzplattformen, Netzinfrastrukturen IVBB
Referat I 1.3
Sicherheitskonzepte Sicherheitsberatung
Referat I 1.4
Systemsicherheit, Grundschutz
Referat I 2.1
CERT-Bund, Lagezentrum
Referat I 2.2
Internet-Sicherheitsanalysen und -verfahren
Referat I 2.3
Unterstützung der Strafverfolgungs-behörden,Prävention
Referat I 2.4
Schadprogramme, Computer-Viren
Referat I 2.5
IT-Penetrations-zentrum
Fachbereich II 1
Sicherheit in Netzen
Fachbereich II 2
Kryptologie, wiss. Grundlagen
Referat II 1.1
Sichere Netzkomponenten
Referat II 1.2
Entwicklung von Kryptosystemen
Referat II 1.3
Evaluierung von Kryptosystemen
Referat II 1.4
Schlüsselmittel, IT-Unterstützung
Referat II 2.1
Schlüssel-technologien
Referat II 2.2
Entwicklung kryptogr. Verfahren
Referat II 2.3
Evaluierung kryptogr. Verfahren
Referat II 2.4
Wiss. Grundlagen, Trends
Fachbereich III 1
Abhörsicherheit
Fachbereich III 2
Allemeine IT-Sicherheit
Referat III 1.1
Mobilfunksicherheit
Referat III 1.2
Abstrahlsicherheit
Referat III 1.3
Grundlagen der Lauschabwehr
Referat III 1.4
Lauschabwehr-prüfungen
Referat III 1.4
Materielle Sicherungstechnik
Referat III 2.1
Grundsatz, Öffentlichkeitsarbeit
Referat III 2.2
Zertifizierung, Zulassung
Referat III 2.3
Akkreditierung, Sicherheitskriterien, Schutzprofile
Referat III 2.4
Kritische Infrastrukturen

Inhalt

- **Einführung**
- **Verfügbare SINA Komponenten**
- **SINA Netzwerk Integration**
- **Beispiel Einsatzszenarien**
- **Zusammenfassung**

Einführung

Ausgangslage 1999



- Aus Kostengründen wurde auf eine hohe Netzwerksicherheit in den neuen/vorhandenen Gebäuden in Berlin verzichtet
- Anforderung der Bearbeitung offener/eingestufter Informationen an beliebigen Workstations/Terminals
- Kein zertifiziertes deutsches IP-Kryptosystem verfügbar
- Forderung einer zeitnahen Aufnahme des Wirkbetriebs

Anforderungen aus Sicht der Administration

- IT-System kann nur vertraut werden, wenn es in einer vertrauenswürdigen Umgebung erstellt, konfiguriert und evaluiert wurde.
- System Entwicklung erfordert Zugang zu Hardware Blaupausen, Betriebssystem- und Applikationssoftware Quellcode und Einsatz offener Entwicklungswerkzeuge (z.B. Compiler).
- Integration proprietärer Komponenten sollte nur unter Wahrung der Sicherheitsvorgaben erfolgen (z.B. Kapselung der Anwendung).

Anforderungen aus Sicht der Nutzer

➨ **“Look and feel” und TCO bei der Verarbeitung eingestufter und offener Informationen sollte (annähernd) gleich sein**

- Nur sogenannte COTS Komponenten, wenn möglich
- Keine separate Netzwerk Installation
- Kein “approved circuit”
- Vertretbarer Einweisungs- und Fortbildungsaufwand
- Vergeichbare Innovationszyklen
- Weitgehende Plattformunabhängigkeit der Anwendungen

SINA Kurzbeschreibung

- Moderne IT-Architektur für sichere Informationsverarbeitung
- Familie modularer und skalierbarer Komponenten für unterschiedliche Einsatzszenarien
- IT-System für sichere Verarbeitung und Übertragung eingestufter Informationen über offene Netze

Sicherheitsmerkmale

- **Netzwerk Sicherheit**
  - IPSec/IKE VPN (sicherheitsoptimiert)
  - Netzwerk Audit und Response
  - Sicherheits-Management (PKI, ACL/Config Man.)
- **Plattform Sicherheit**
  - SINA-Linux (gehärtet)
  - Virtual Machine (VM) Technologie
  - Krypto-Dateisystem
- **Sicherheitskomponenten**
  - Smart Card Technologie
  - PEPP1 Kryptokarte mit “PLUTO”-Chip
  - Generisches Kryptointerface (für SW/HW-Kryptographie)

SINA Projekt Meilensteine

- **1999:** Entwicklung eines Prototypen und Projektstart durch das BSI
- **Q1/2000**: Beginn SINA (Secunet AG) und Kryptokarte “PEPP1” (Rohde und Schwarz – SIT) Entwicklung
- **Q4/2000**: SINA-Box-S (Zulassung für “VS-VERTRAULICH”)
- **Q4/2001**: SINA-Thin-Client-S (Zulassung für “VS-VERTRAULICH”)
- **Q1/2002**: Beginn SINA-Virtual-Workstation Entwicklung
- **Q3/2002**: SINA-Box-P mit Kryptocard PEPP1 und Kryptochip “PLUTO” verfügbar (vorläufige Zulassung für GEHEIM)
- **Q1/2003**: SINA-Box-P mit Kryptokarte PEPP1 and Kryptochip “PLUTO” erhält die endgültige Zulassung für GEHEIM
- **Q2/2003**: Beginn “Encapsulated Encrypted Server” Entwicklung
- **Q4/2003**: SINA-Box-H (Zulassung für STRENG GEHEIM)

Verfügbare

SINA-Komponenten

Verfügbare Komponenten

➜ **SINA Linux:** Gehärtete und minimalisierte Linux System Plattform

➜ **SINA Box:** Klassisches IPSec VPN-Gateway

zugelassen durch das BSI für die Verarbeitung eingestufter Daten bis einschliesslich "**STRENG GEHEIM**" (10/2003)

➜ **SINA Thin-Client:** Terminal-Server basierte Online Informationsverarbeitung für das Thin-Client/Server Szenario

zugelassen durch das BSI für die Verarbeitung eingestufter Daten bis einschliesslich "**STRENG GEHEIM**" (10/2003)

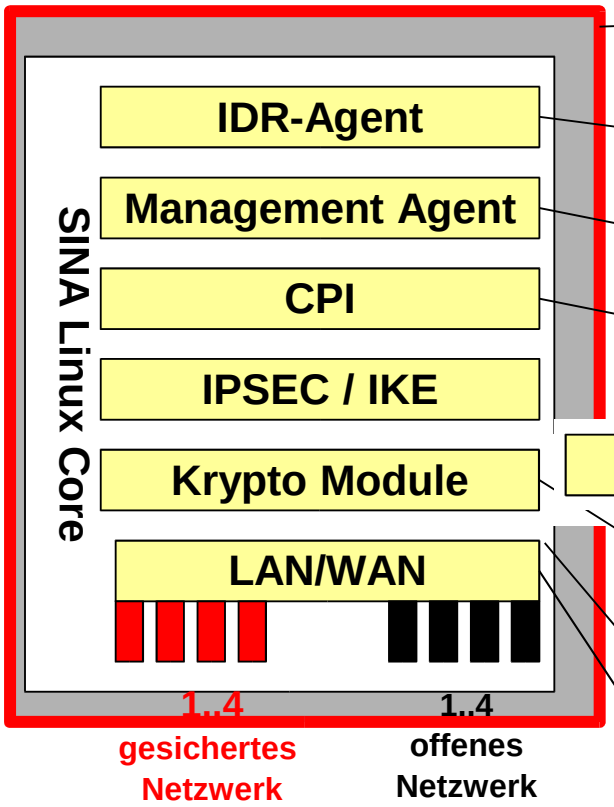
➜ **SINA Virtual Workstation:** Gekapselte Informationsverarbeitung

verfügbar: **Q1/2005**

➜ **SINA Management:** PKI - basiertes Konfigurations- und Sicherheitsmanagement

➜ **Spezialanfertigungen:** Datendiode, Encapsulated Encrypted Server (EES) (Q2/2004), SINA-Cluster, ...

SINA-Box



- Tamperschutz und Schutz gegen kompromittierende Abstrahlung (Tempest)
- Intrusion Detection System
- Sichere Schnittstelle zum Management
- generisches Crypto Provider Interface (CPI)
- Smartcard/USB token (EC-DSA or RSA basiert)
- PEPP1 Kryptokarte mit “PLUTO”-Chip Software Module (AES, 3DES, Chiassmus, ...)
- Minimalisierte und gehärtete (SINA-) Linux Plattform wird von CDROM oder FLASH geladen
- Optische LAN/WAN Schnittstelle

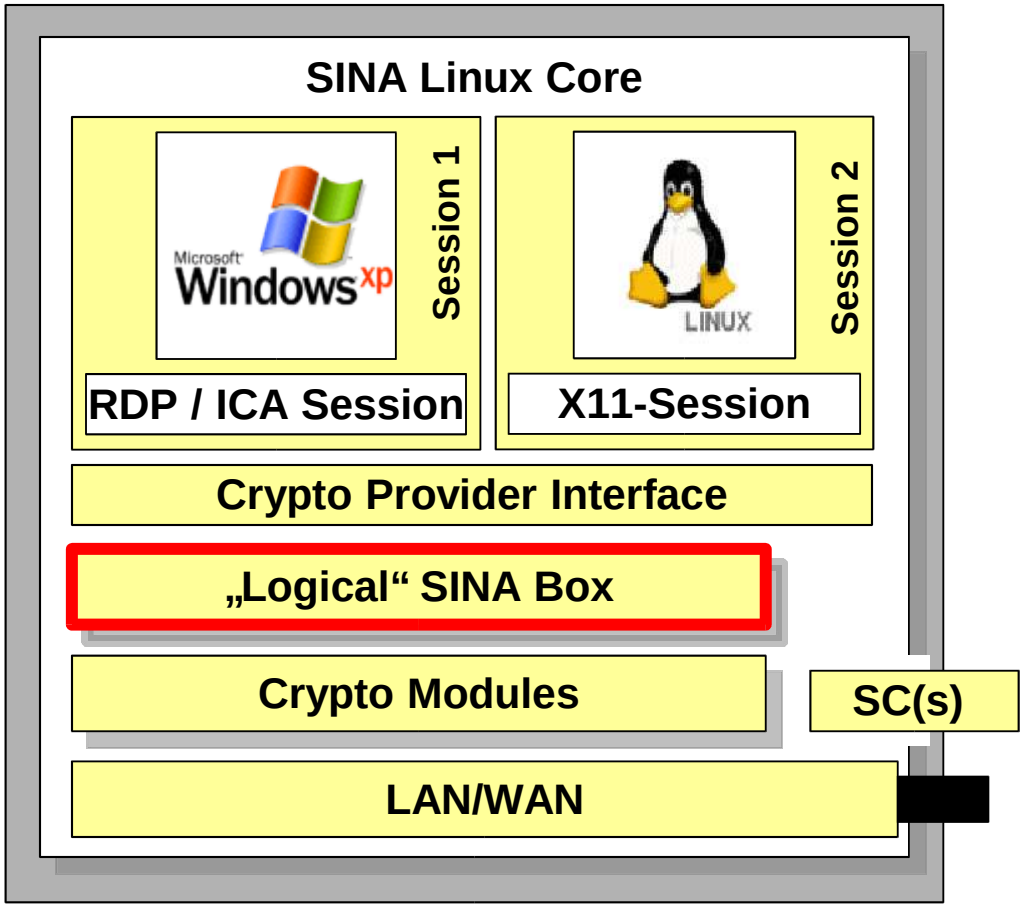
Thin-Client

- **Thin-client/server architecture**
- **Supported terminal server sessions:**

  RDP **: Microsoft Remote Desktop Protocol Version 4, Soon 5.x for XP**

  ICA **: MetaFrame CITRIX Independent Computing Architecture**

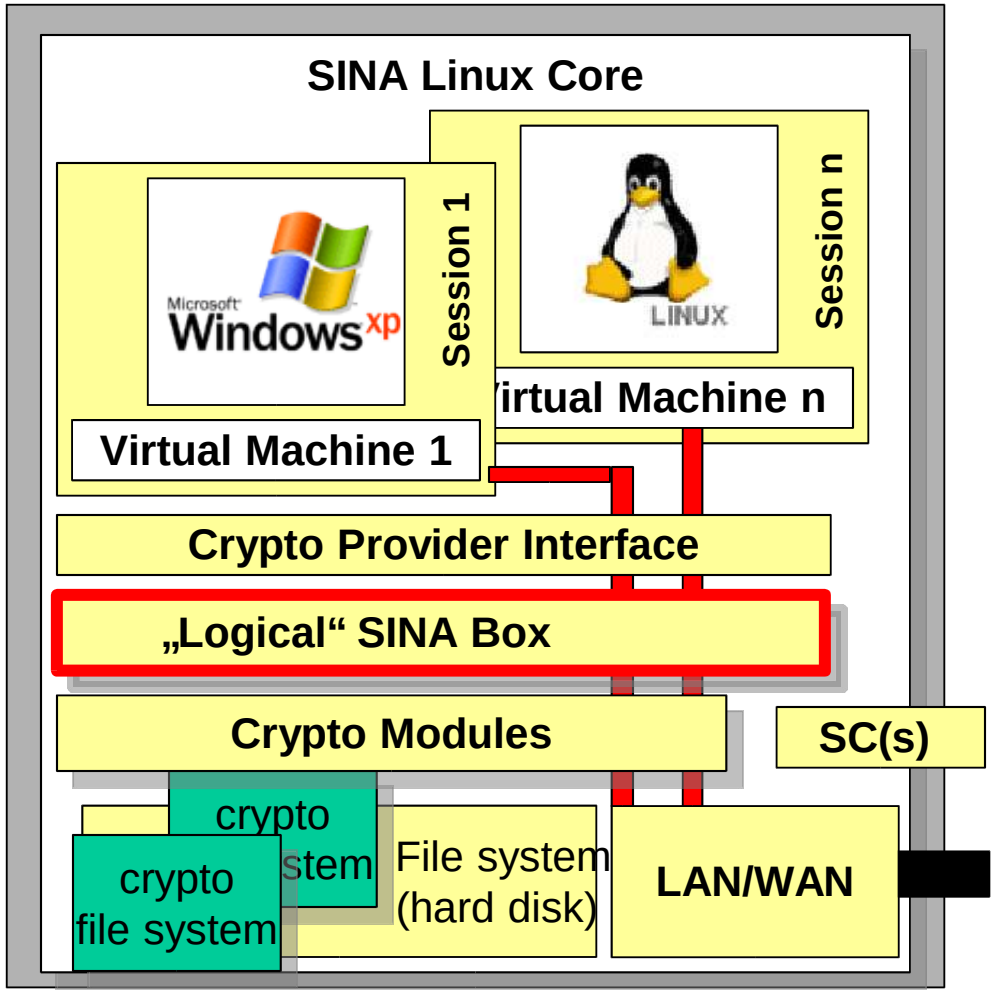
  X11/XDMCP**: any UNIX**



SINA Virtual Workstation

Server Betriebssysteme werden vollständig durch das SINA System gekapselt

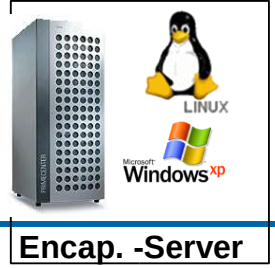
Vertrauliche Daten liegen in einem Kryptographischen Dateisystem

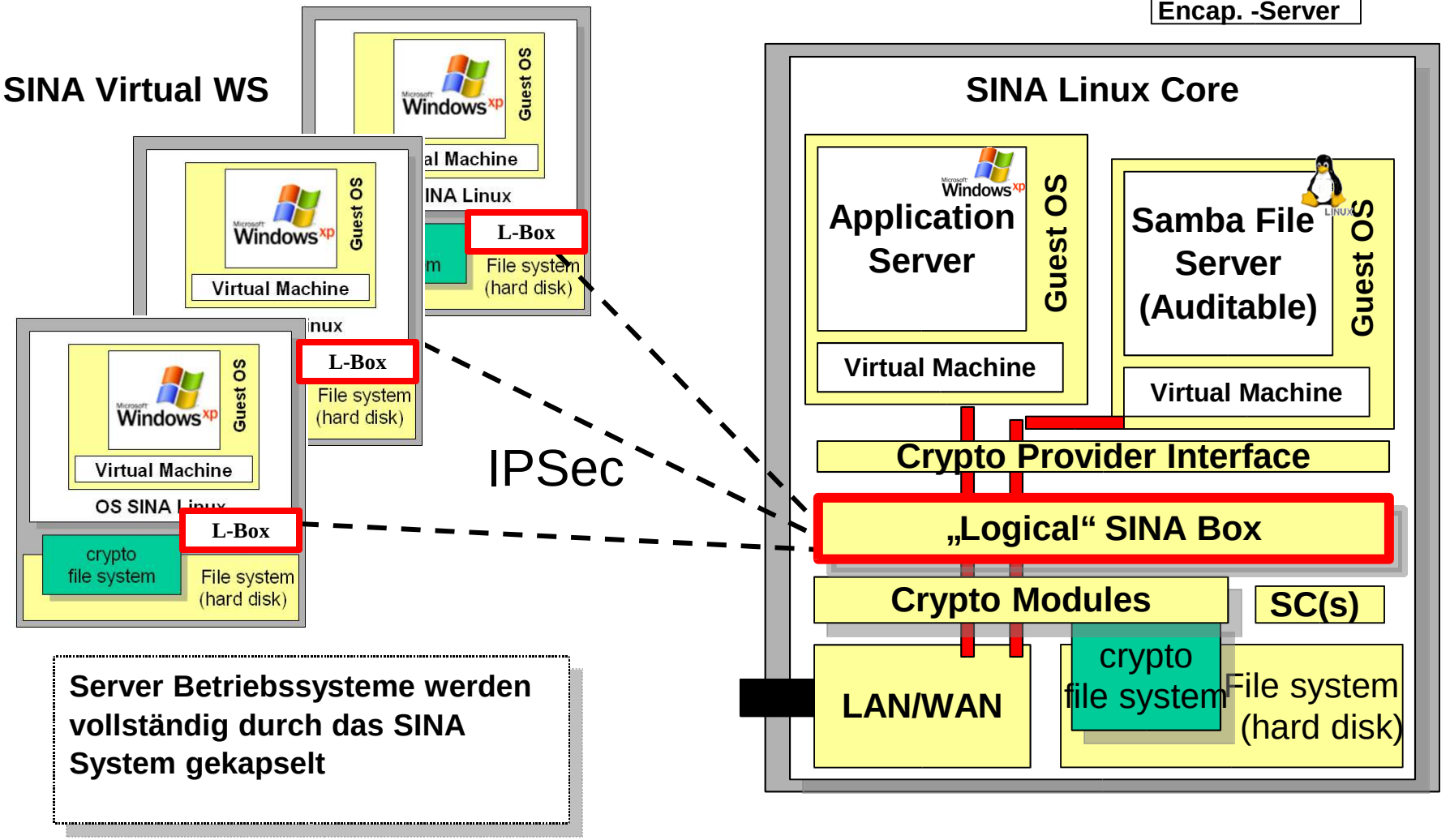


Virtual Machine

vmware

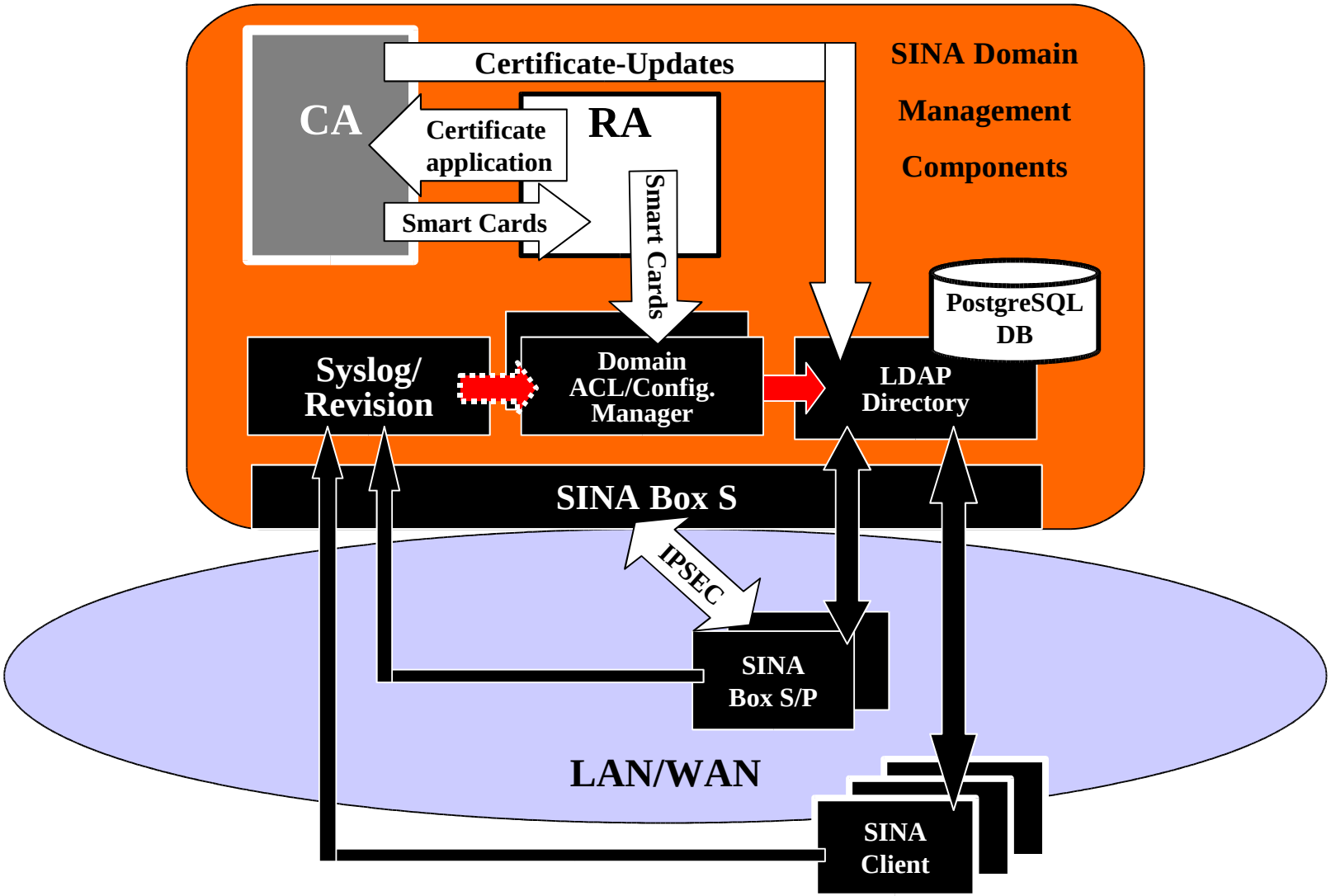
Encapsulated Encrypted Server





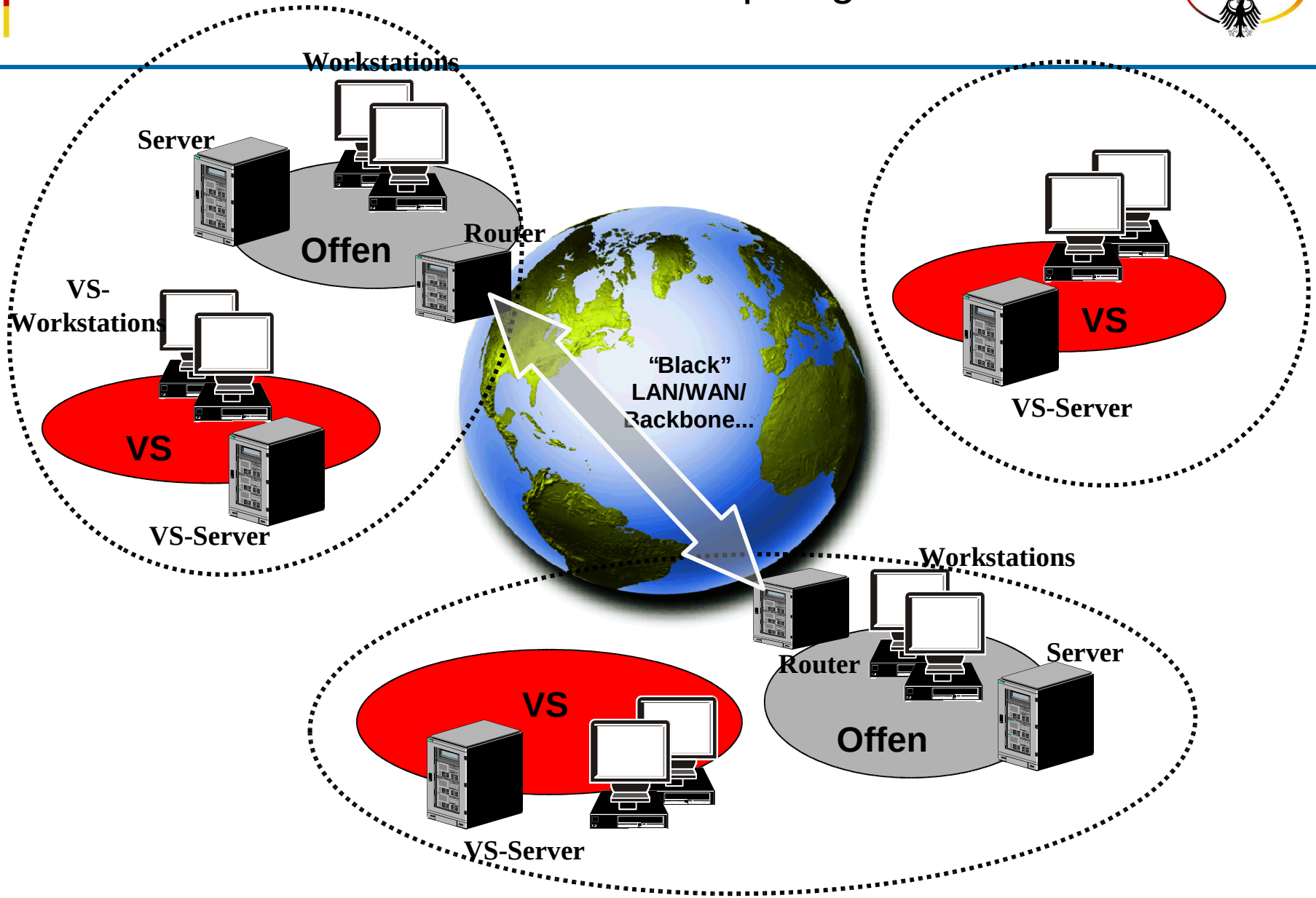
Server Betriebssysteme werden vollständig durch das SINA System gekapselt

SINA Management



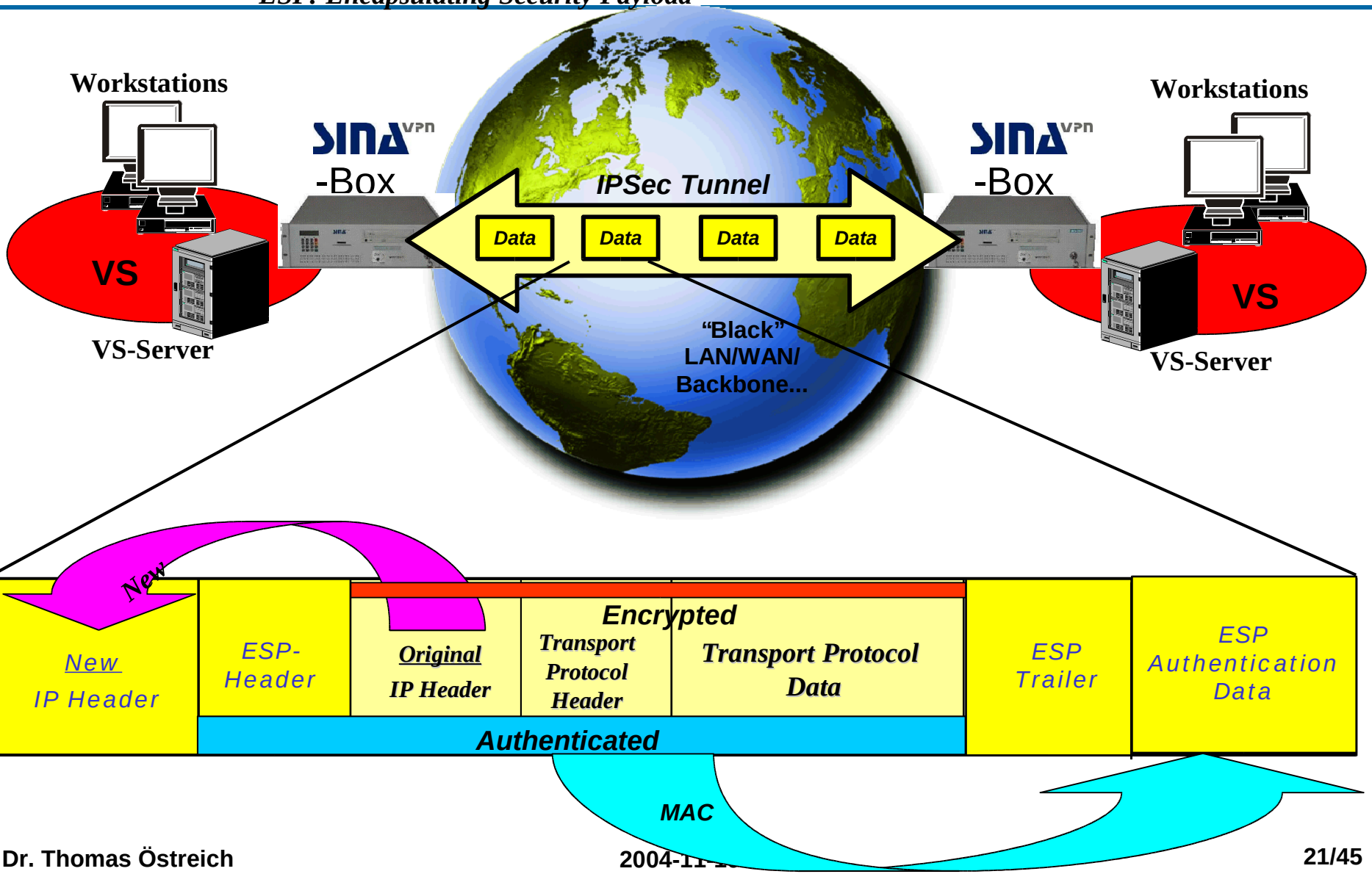
SINA-Netzwerk Integration

Klassische Netzwerk Topologie ohne SINA

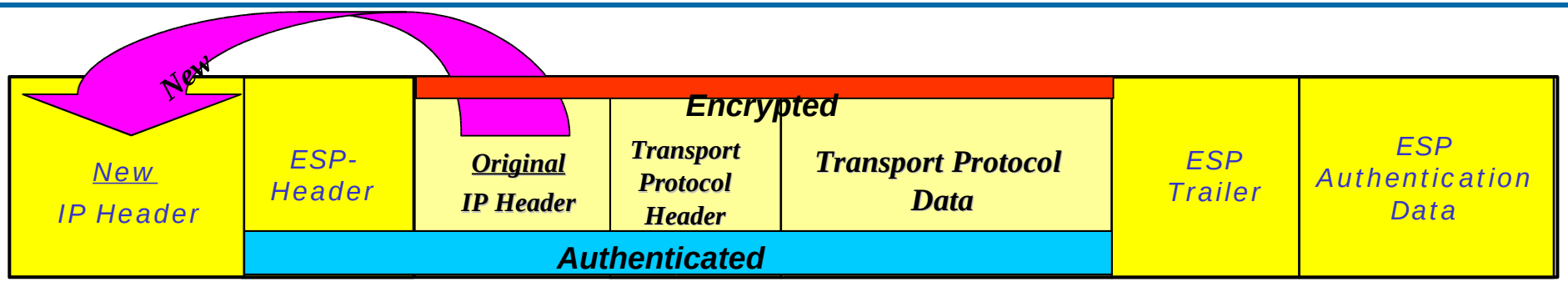


IPSec Tunnel: ESP-Tunnel Modus

ESP: Encapsulating Security Payload

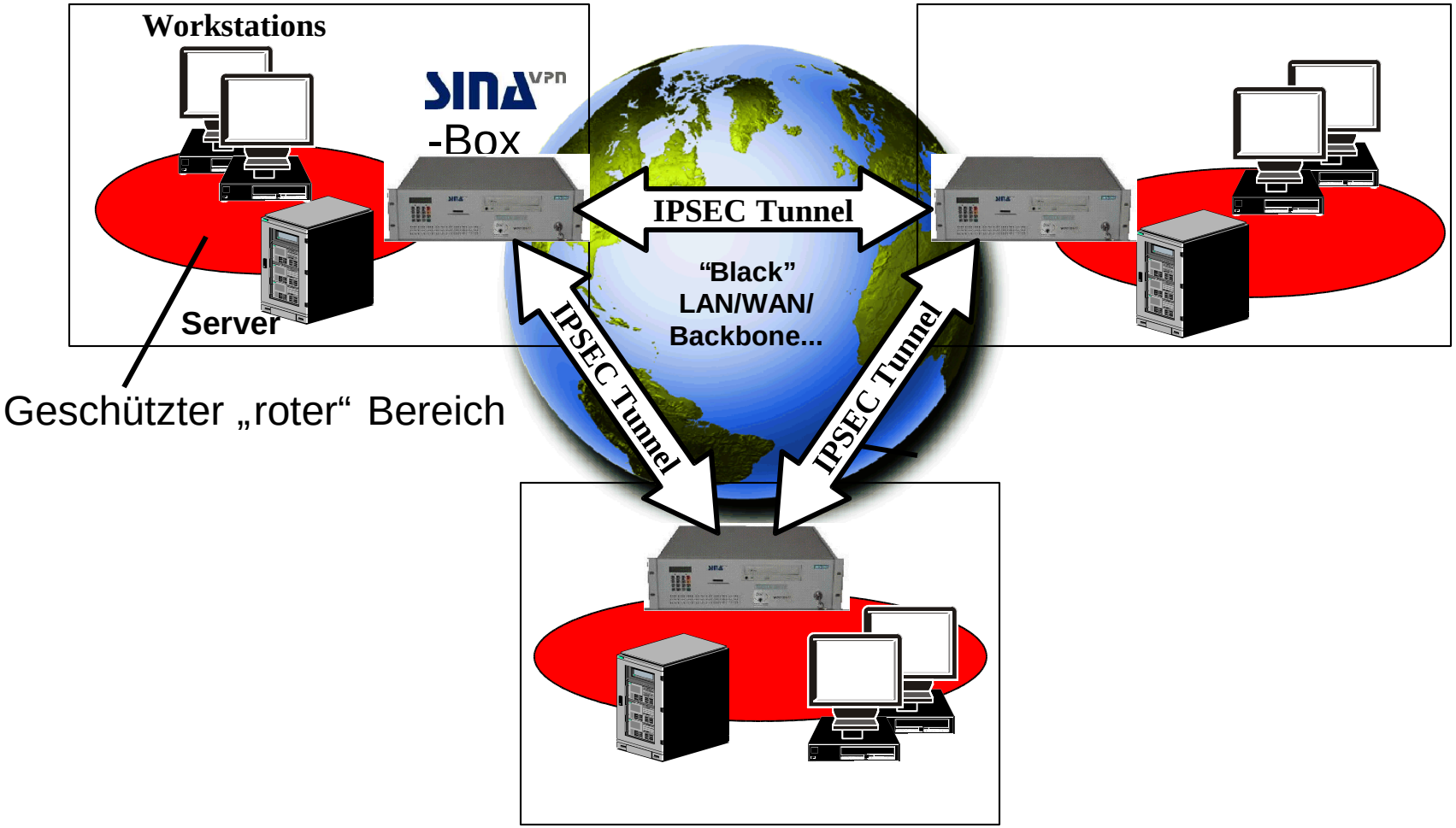


ESP Schutzmechanismen

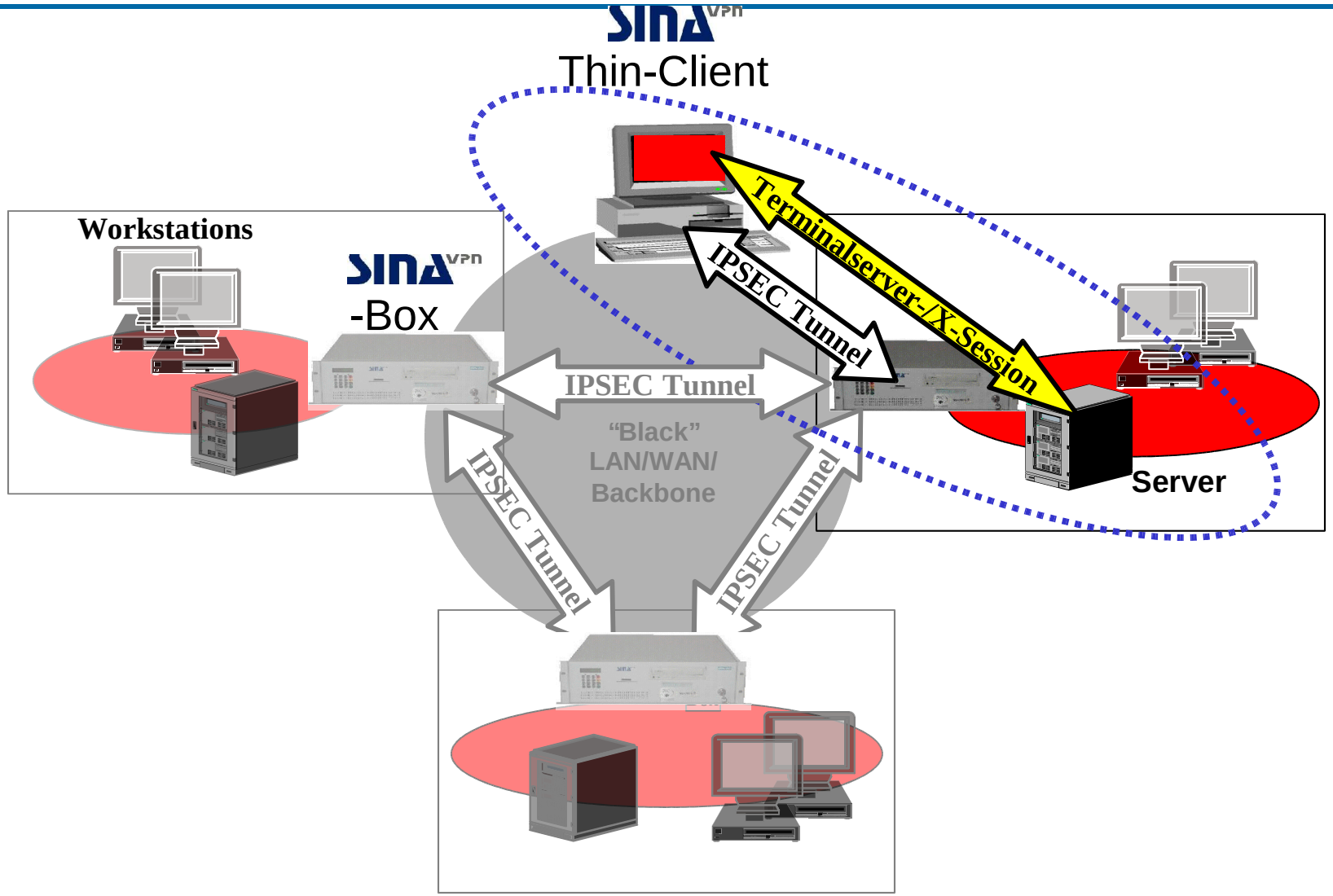


- Vertraulichkeit des Datenfluß
  (Verschlüsselung und Kapselung des vollständigen IP Pakets)
- Verbindungslose Sicherheit
  (Integritätsprüfung via MAC einzelner IP Datagramme)
- Authentizität des Datenursprungs
  (Verifizierung and Authentifizierung des Datensenders)
- Wiedereinspiel-Schutz
  (ESP-Protokollkopf enthält 32 Bit Sequence Number)

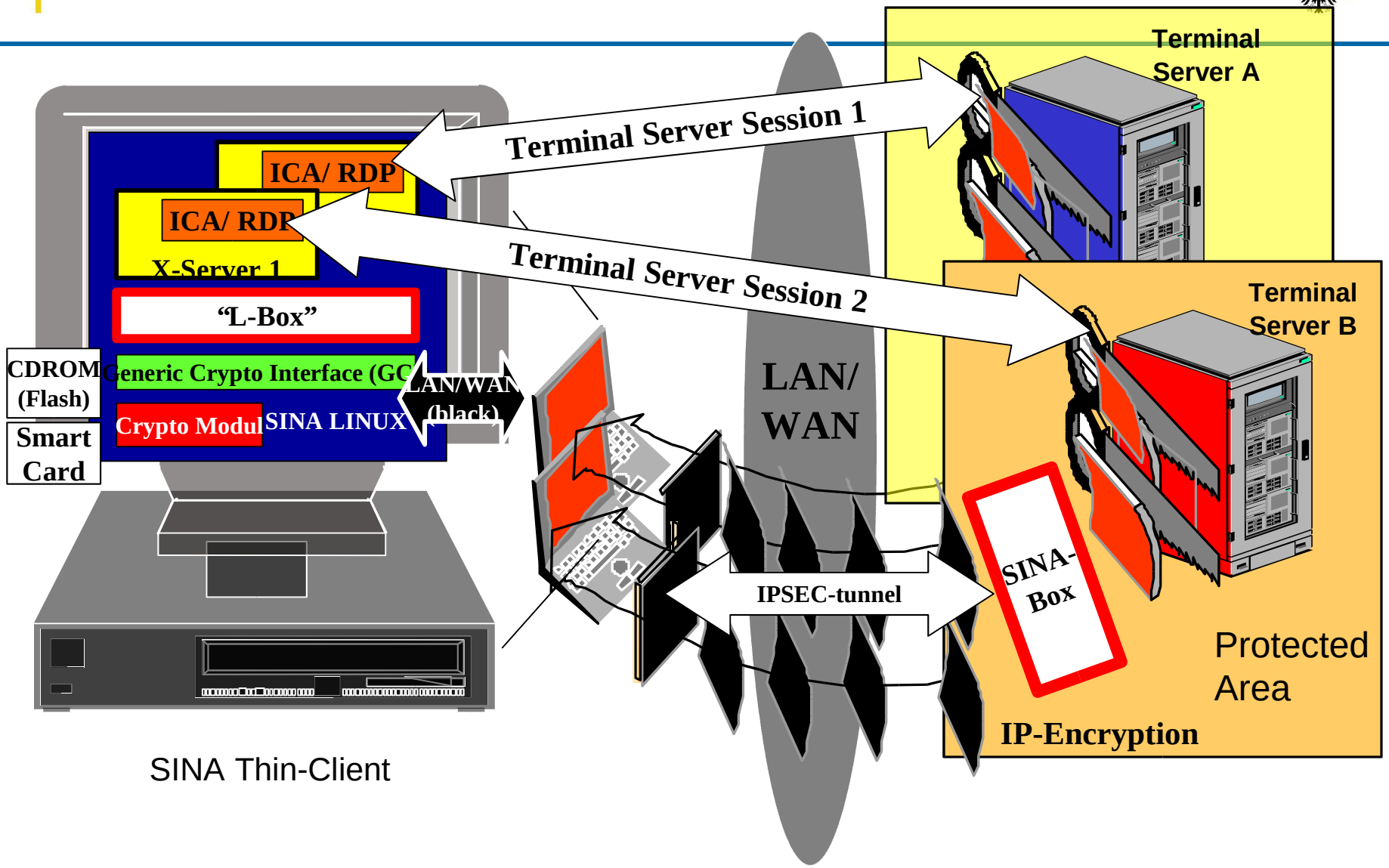
Klassisches VPN Szenario mit SINA-Boxen



Thin-Client Integration

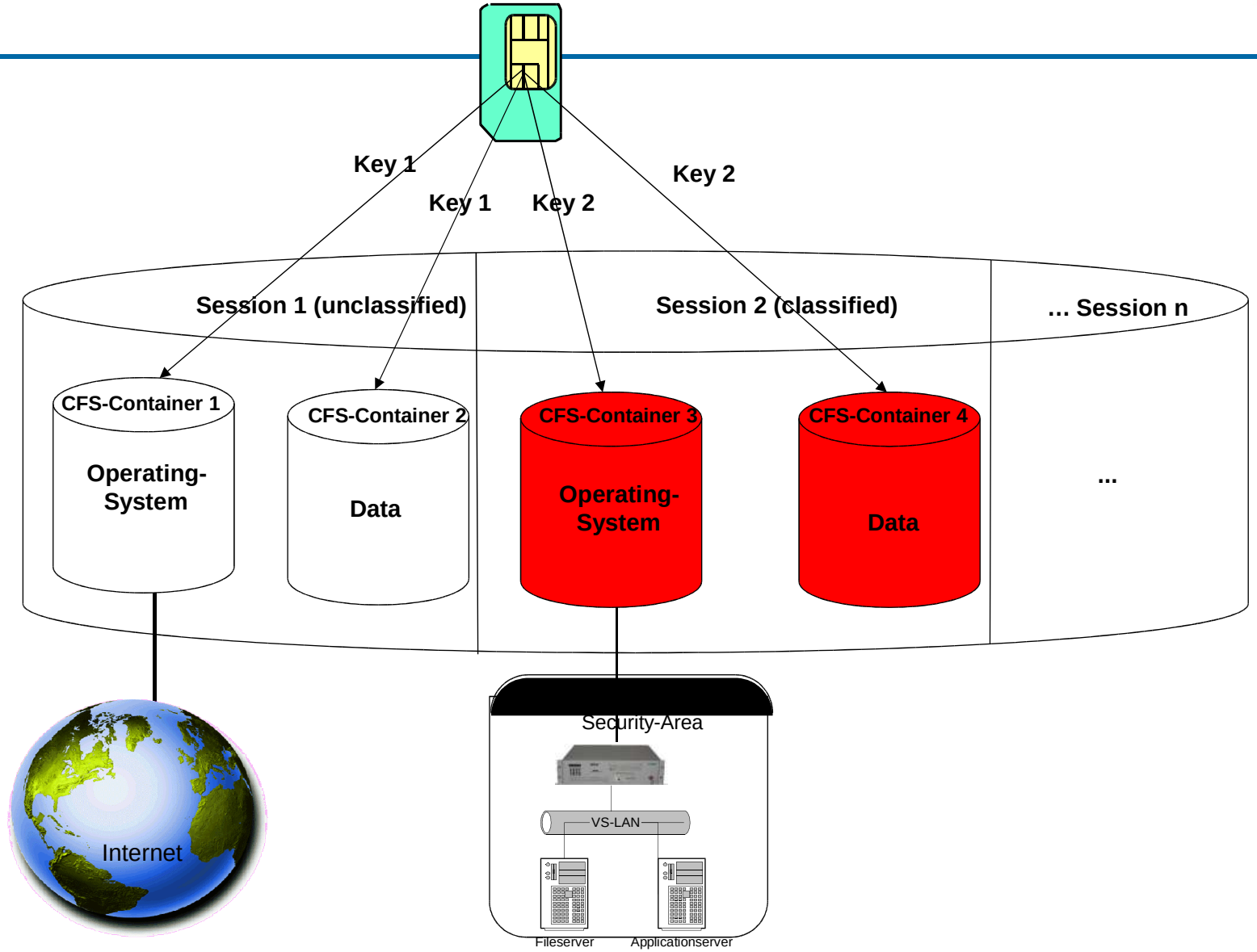


Client/Server Computing (Prinzip)



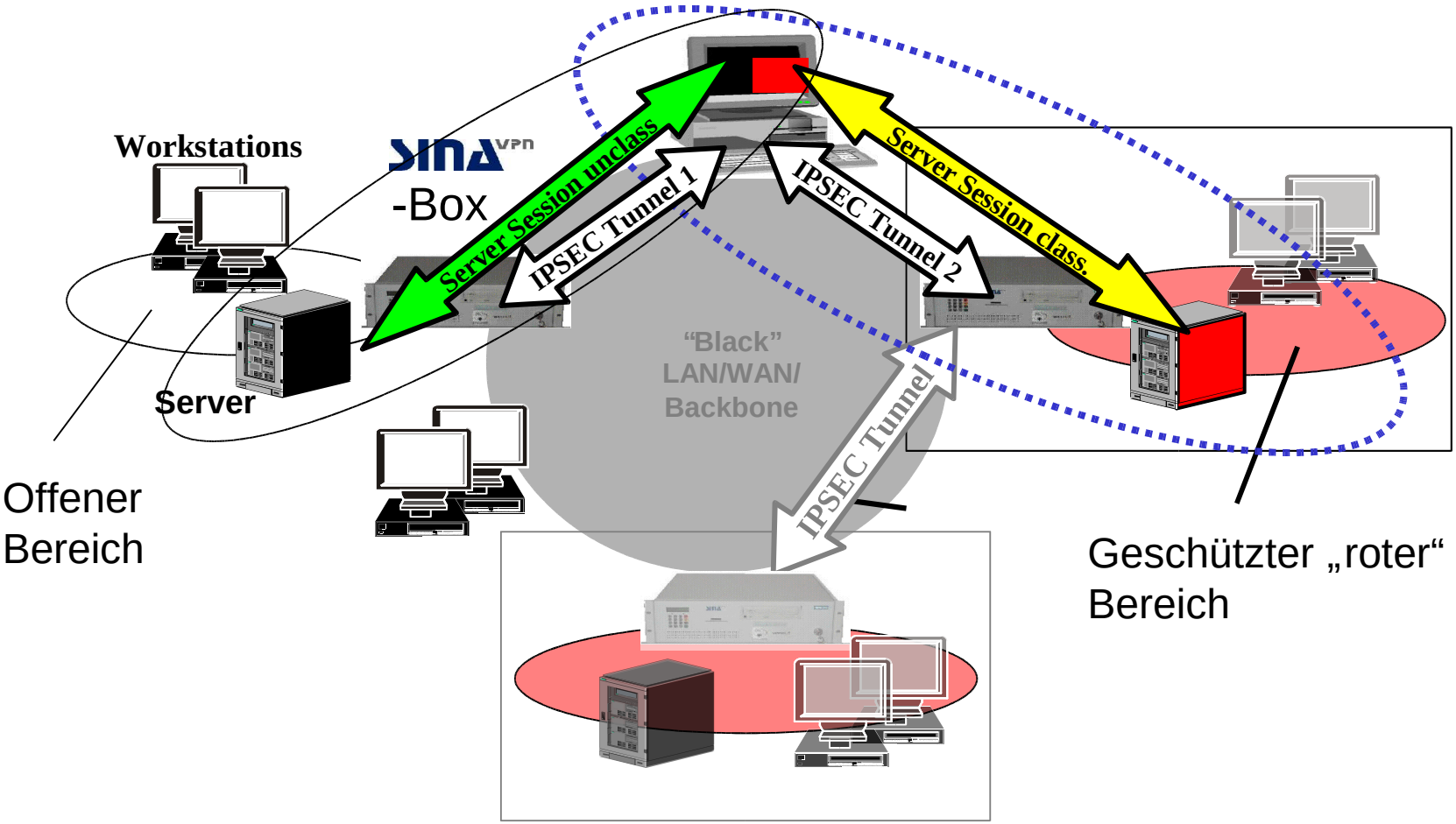
SINA Thin-Client

Kryptographisches Dateisystem (CFS)

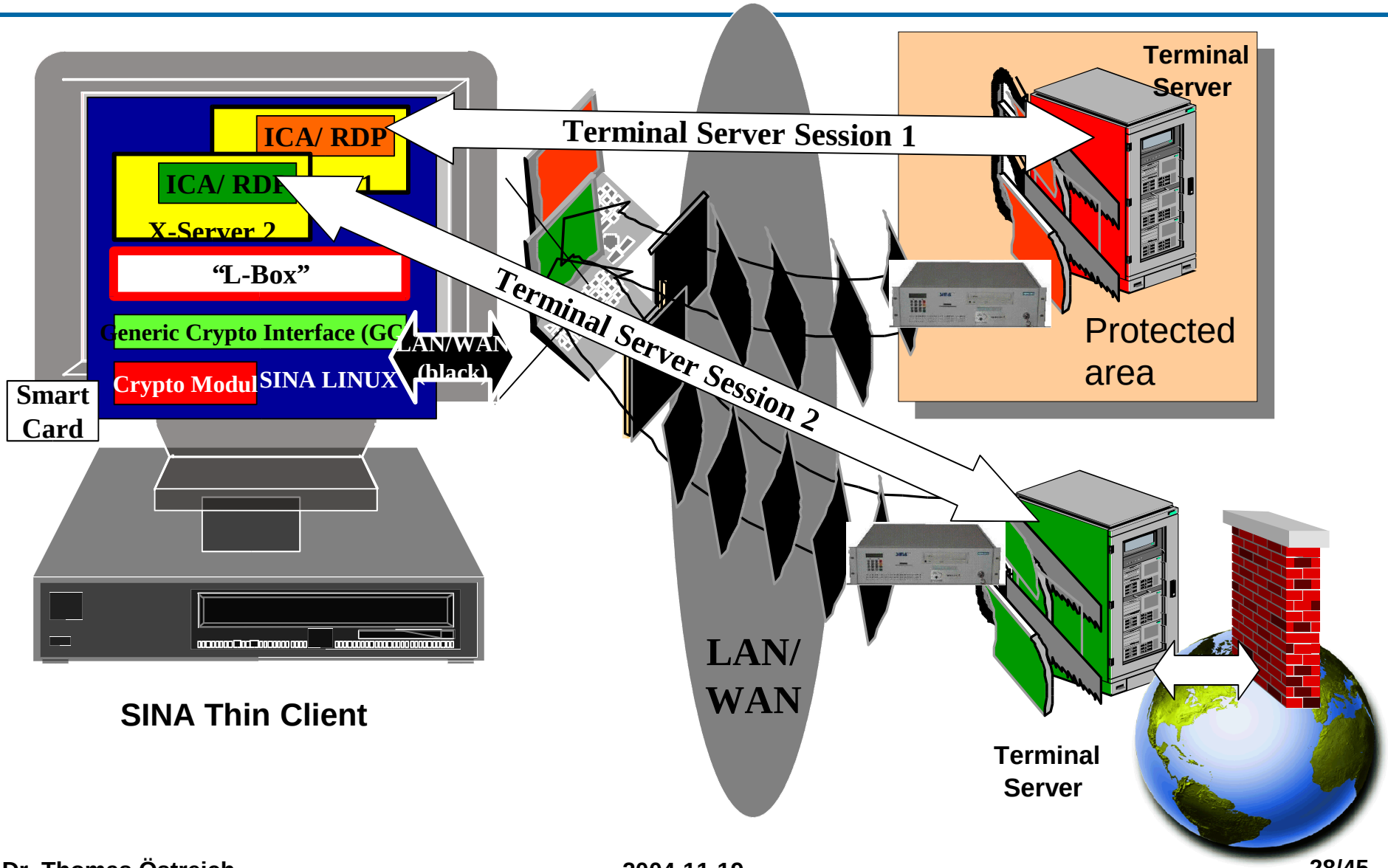


“Gekapselte” Informationsverarbeitung

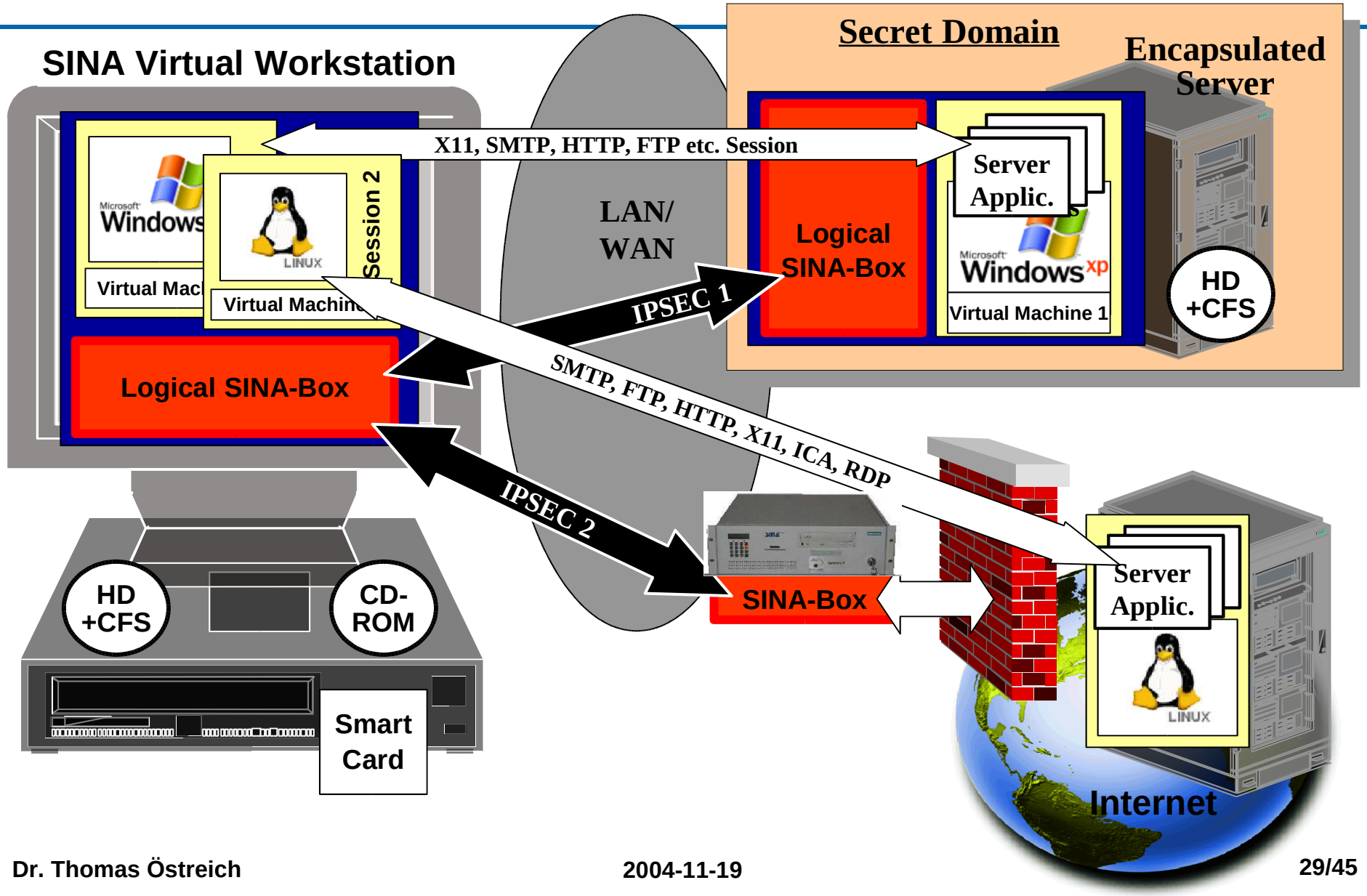
„Kapselung“
Thin-Client oder Virtual Workstation



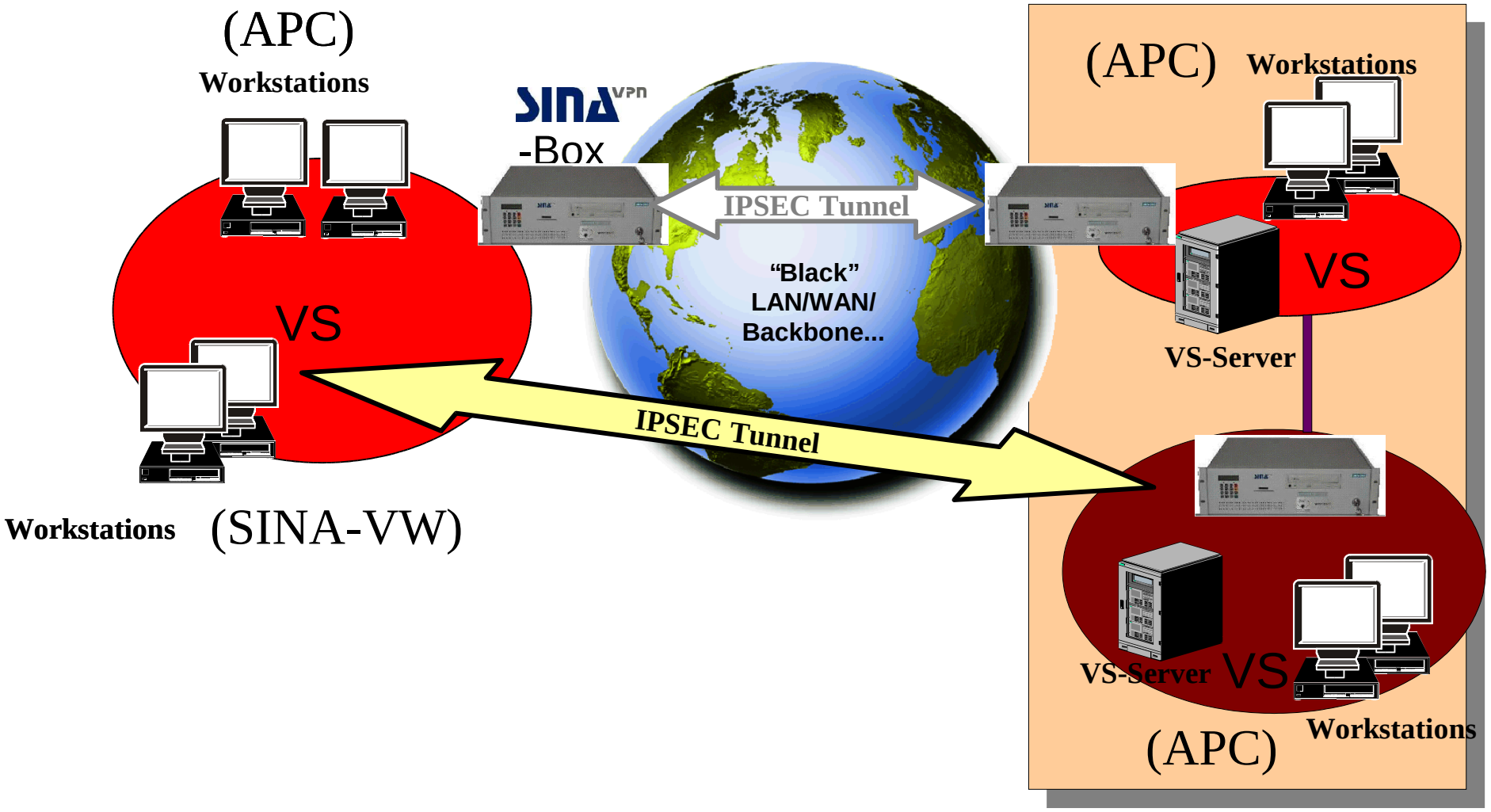
“SINA-Invers” Einsatzszenario



Kapselung im Virtual Workstation Einsatz



VPN Doppel-Tunnel Aufbau

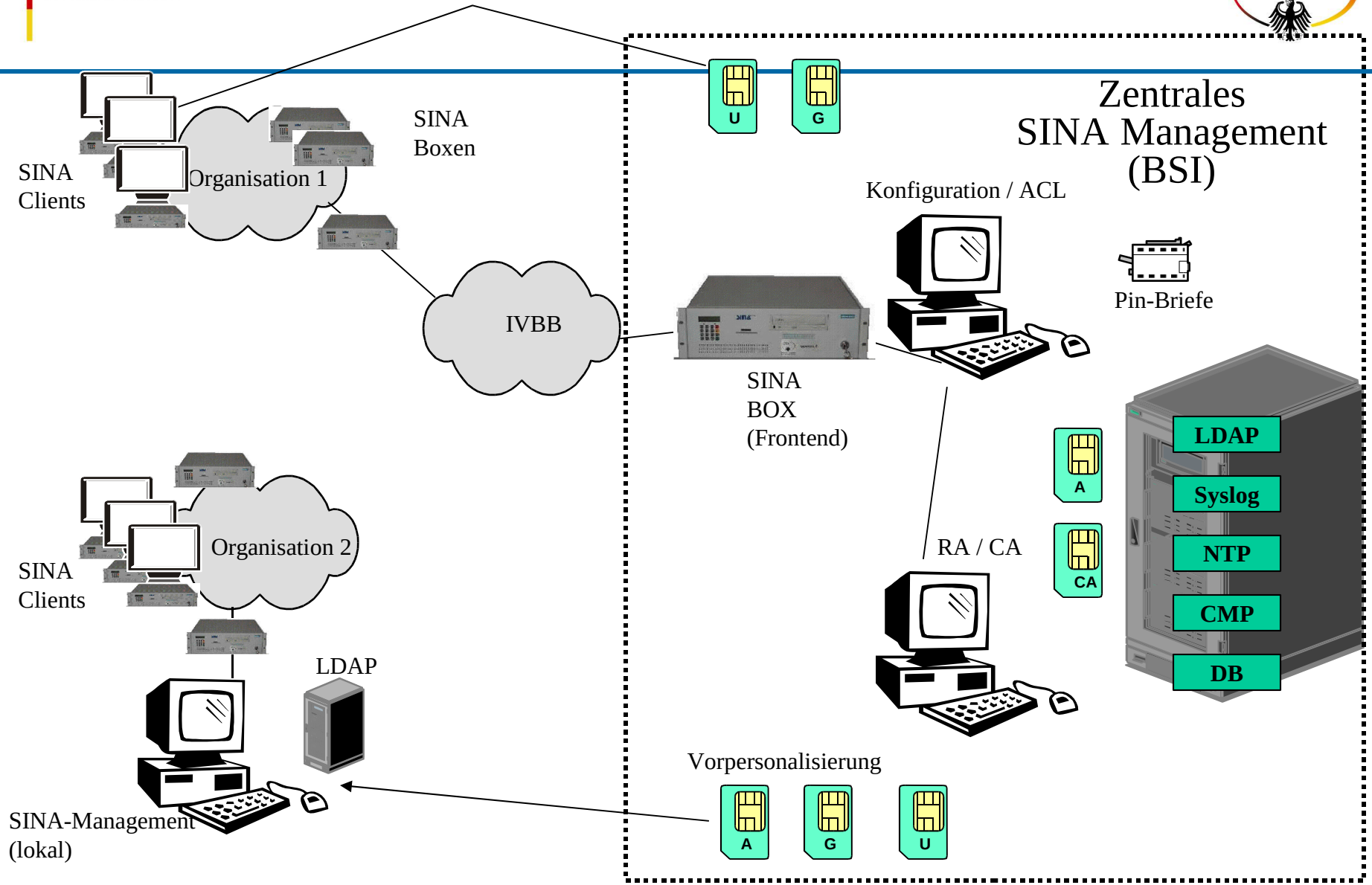


BSI Vorgaben für eine Zulassung

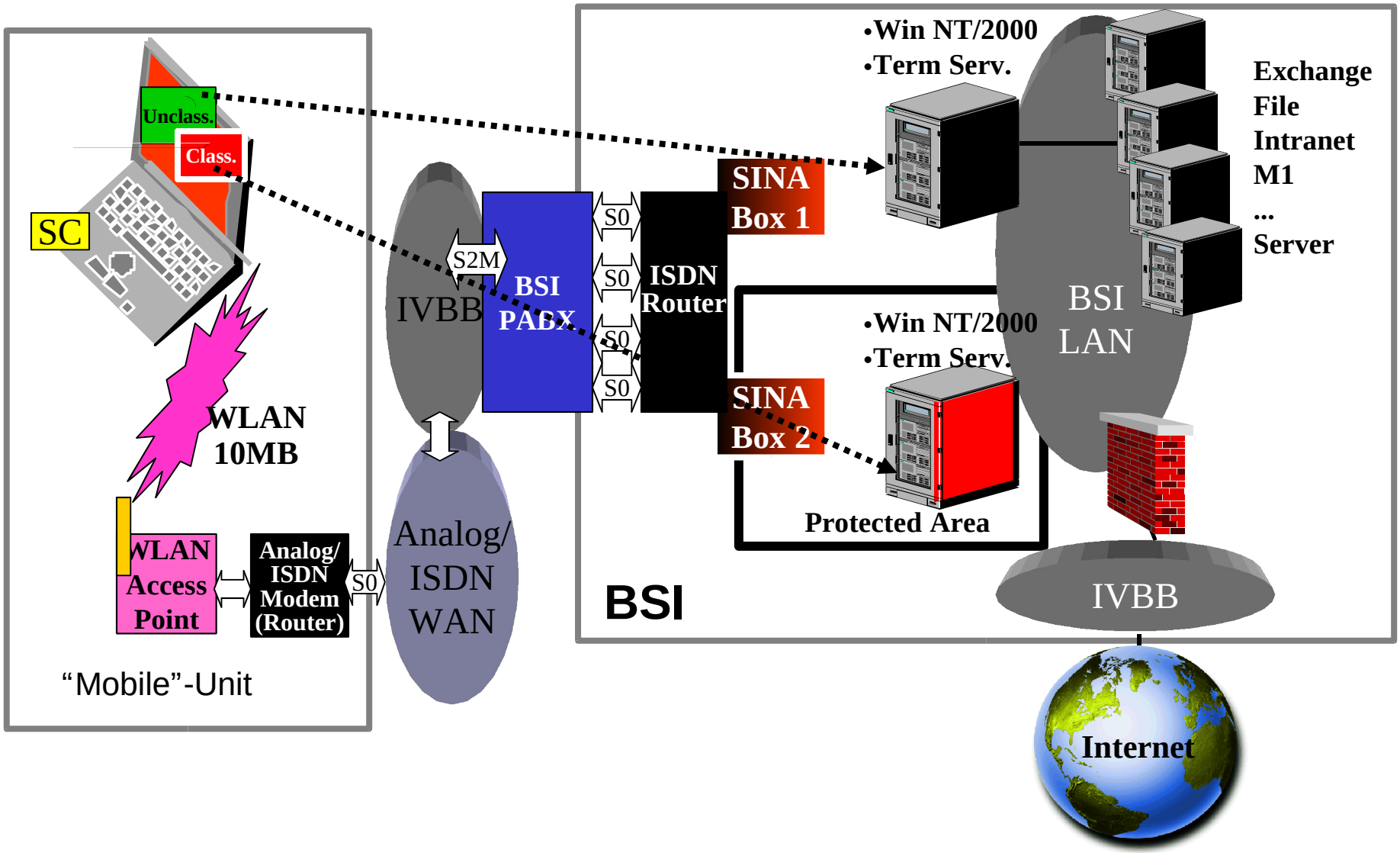
Geheim-haltungs-stufe	(VS-)								NATO					
	NfD		VERTRAU-LICH		GEHEIM		STRENG GEHEIM		RESTRICTED		CONFIDENTIAL		SECRET	
Netzintegration	LAN	WAN	LAN	WAN	LAN	WAN	LAN	WAN	LAN	WAN	LAN	WAN	LAN	WAN
TEMPEST	unverzont		Zone 1					Zone0	unverzont		Zone 1		Zone 0	
Antitamper	nein		ja						nein		ja			
galvanische Trennung	nein		ja						nein		ja			
symmetr. Krypto	≥AES		≥XIA		≥XIA		Libelle		≥AES		Libelle			

Beispiel Einsatz-szenarien

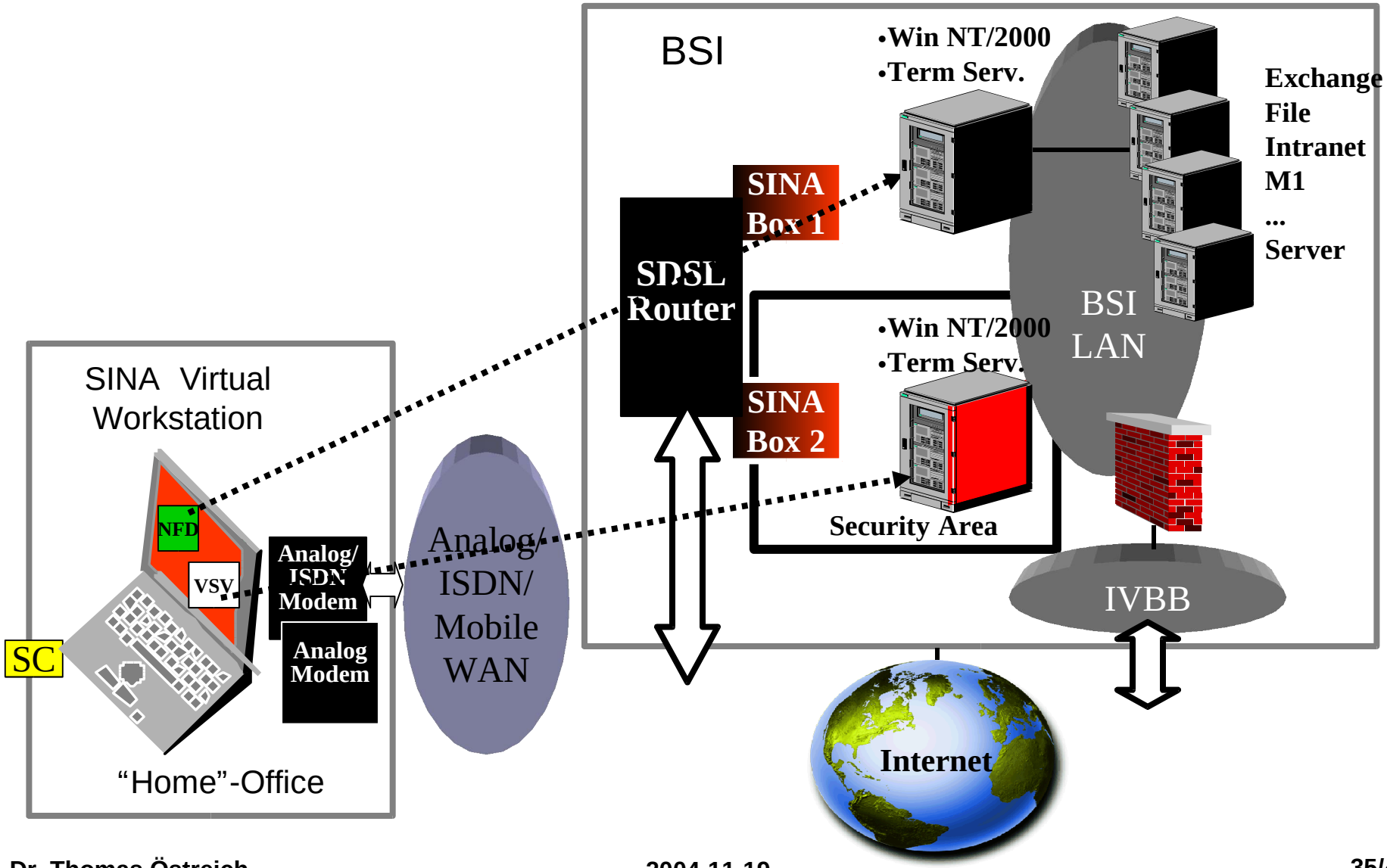
Management Szenarien



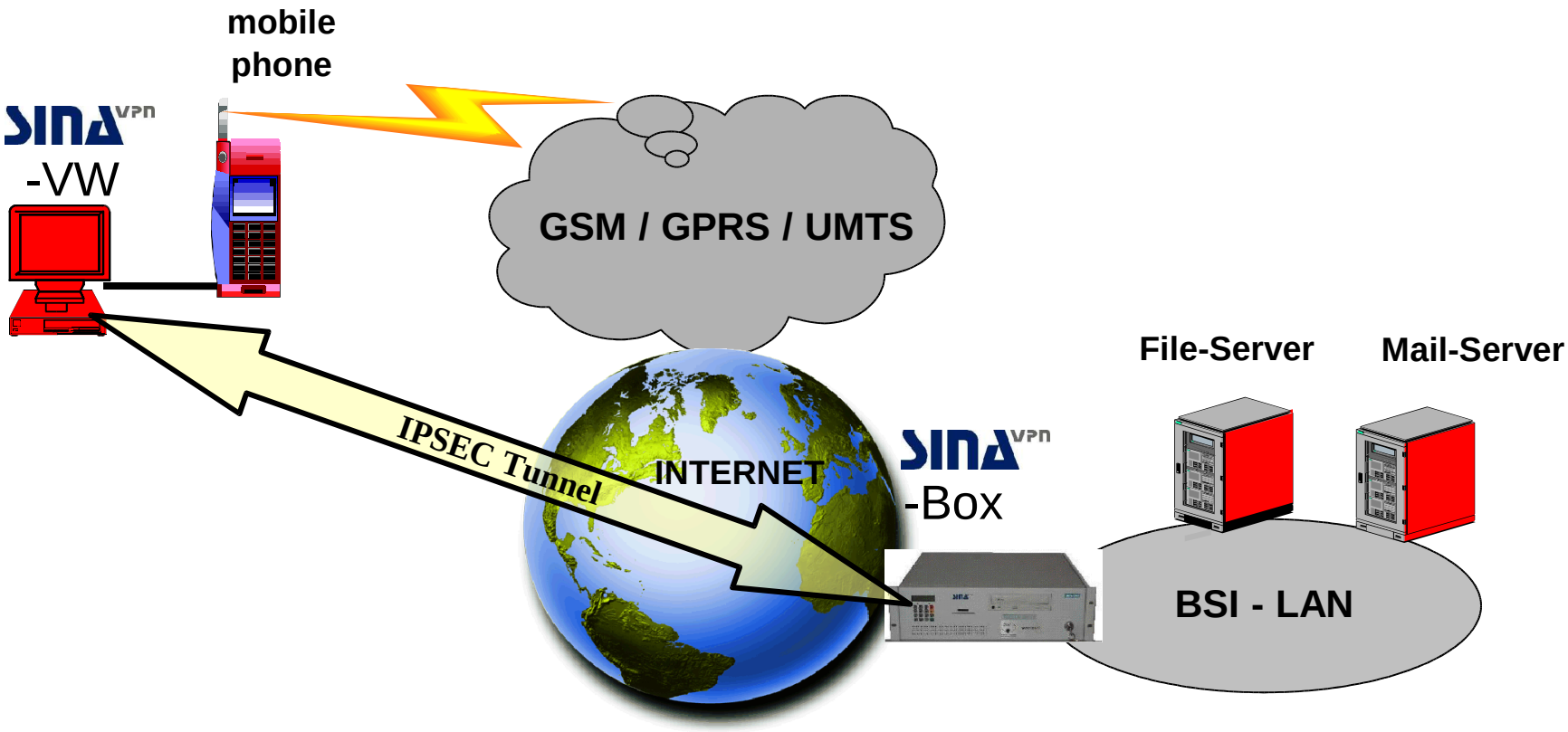
Remote Access (Analog/ISDN)



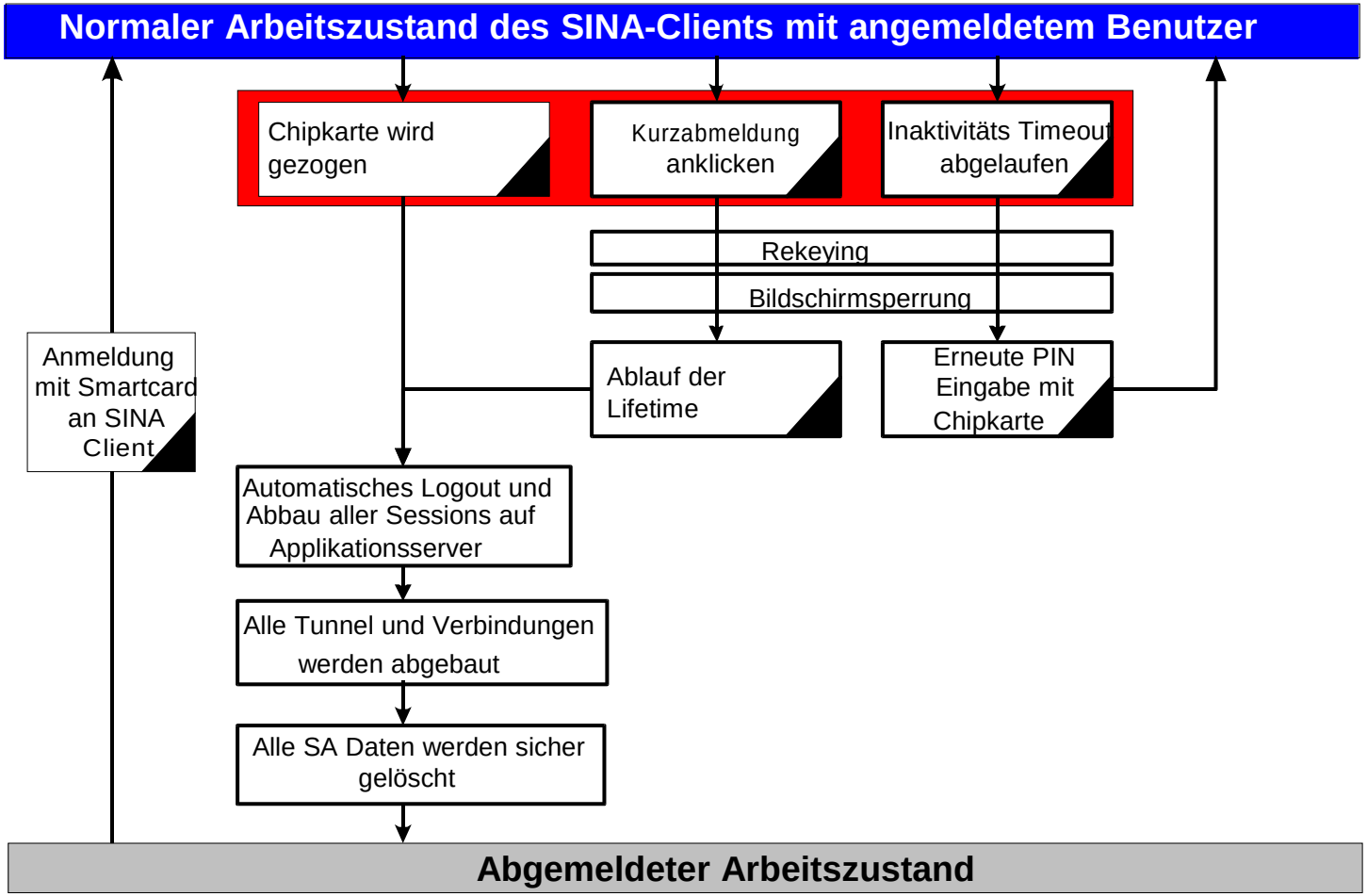
Remote Access über ISP



“Mobilität” der SINA-Virtual-Workstation



Sperrung der SINA Konsole



Zusammenfassung

SINA-Box Performanz Daten

- Stark abhängig von:
  - ausgewähltem (symmetrischen) Kryptoalgorithmus
  - Länge der Datenpakete (Applikation)
  - Anzahl der (IPSec-)Security Associations (SA) mit weiteren verbundenen SINA-Boxen und SINA-Thin-Clients
- Beispiel Datendurchsatz:
  - 80 MBit/s (Hardware Version PEPP1-Board inkl. PLUTO-Chip)
  - 50 MBit/s (Pentium III mit 866 MHz) mit SW-AES (192 Bit)
  - 150 MBit/s (Dual Xeon System) mit SW-AES (192 Bit)
- Skaliert mit CPU Leistung und PC-Hardware
- Beliebige Skalierung mit Einrichtung von „Load Balancing“

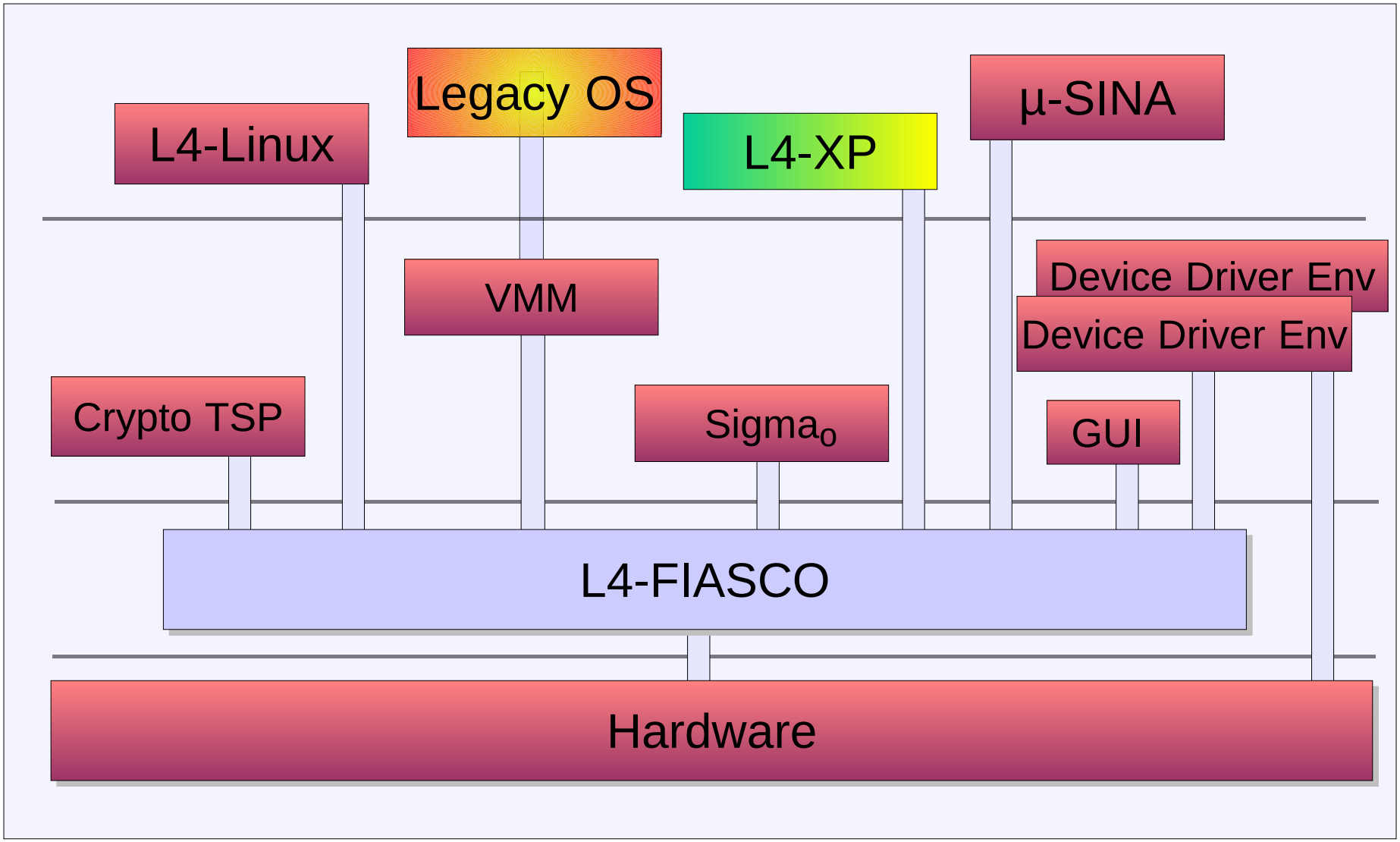
Einsatzbeispiele

- LfV Hamburg, Bayern, Mecklenburg-Vorpommern
  (Clients und Boxen, seit I/2002)
- BGS, zunächst nur WAN (seit I/2002),
  im LAN-Bereich später geplant
- Auswärtiges Amt
  (SINA-Boxen mit Spezialroutern, SINA-VW-Tests)
- Bundeskanzleramt
  (Dual-Boot Clients, Boxen, VS-FileServer seit 09/2002)
- IVBB: Load Balancing Cluster an Kopfstellen
  (Berlin, Bonn, im Pilotbetrieb)
- Generalsekretariat EU (Testbetrieb, seit 09/2002)

Ausblick

- Erweiterte Managementfunktionen
- USB - Firewall
- QoS - Priorisierung von Datenströmen auf der SINA-Box
- DHCP - Unterstützung
- Secure Workflow Komponente
- SINA Mikrokern Sicherheitsplattform
- IPv6
- Healthmonitor
- Backup Routing

Mikrokern Plattform



Zusammenfassung

- Bewahrung des „Look and Feel“ der gewohnten Desktop Umgebung
- Flexible und schnelle Verarbeitung vertraulicher Informationen
- Zugriff auf sensitive Daten ohne die Notwendigkeit einer lokalen Kopie
  - minimiert Daten- und Hardwarediebstahl
- Sichere Übertragung eingestufter Informationen über unsichere offene Netze
  - gewährleistet die Vertraulichkeit und Integrität sensitiver Daten
- VPN-Technologie erfordert keine zusätzliche physikalische Netzwerkabsicherung
- Beschaffung dedizierter Kryptogeräte entfällt
- Unterstützung kurzer IT-Innovationszyklen
- Niedrige „Total Cost of Ownership“ (TCO)

SINA Hardware Komponenten
(z.B. Siemens TEMPEST)

-Box 19“

-Thin Client

-Minibox

Kontakt

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Dr. Thomas Östreich
Godesberger Allee 185-189
53175 Bonn

Tel: +49 (0)1888-9582-466
Fax: +49 (0)1888-9582-90466

thomas.oestreich@bsi.bund.de
www.bsi.bund.de
www.bsi-fuer-buerger.de