

VERTRAULICH

Münchner-Kreis

München, den 18. September 2003

Sichere Kommunikation mit und in der öffentlichen Verwaltung

Was ist sichere Kommunikation / wann ist Kommunikation sicher

Kommunikationsbeispiele:

- Antrag über E-Mail
- Übersendung eines Dokumentes
- Telefongespräch
- Videokonferenz
- Online Chat
- Online Formular

Kommunikation ist sicher, wenn die

- die Authentizität
- die Integrität und
- die Vertraulichkeit

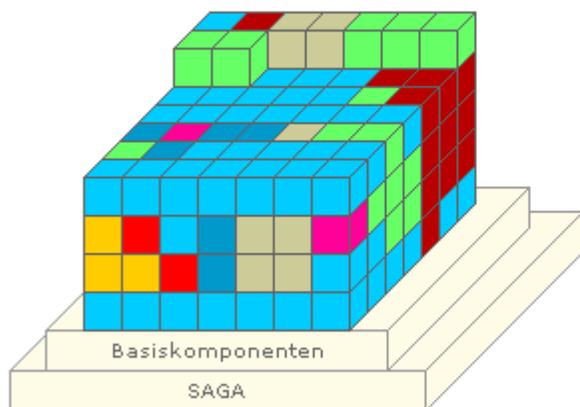
sichergestellt ist.

eGovernment

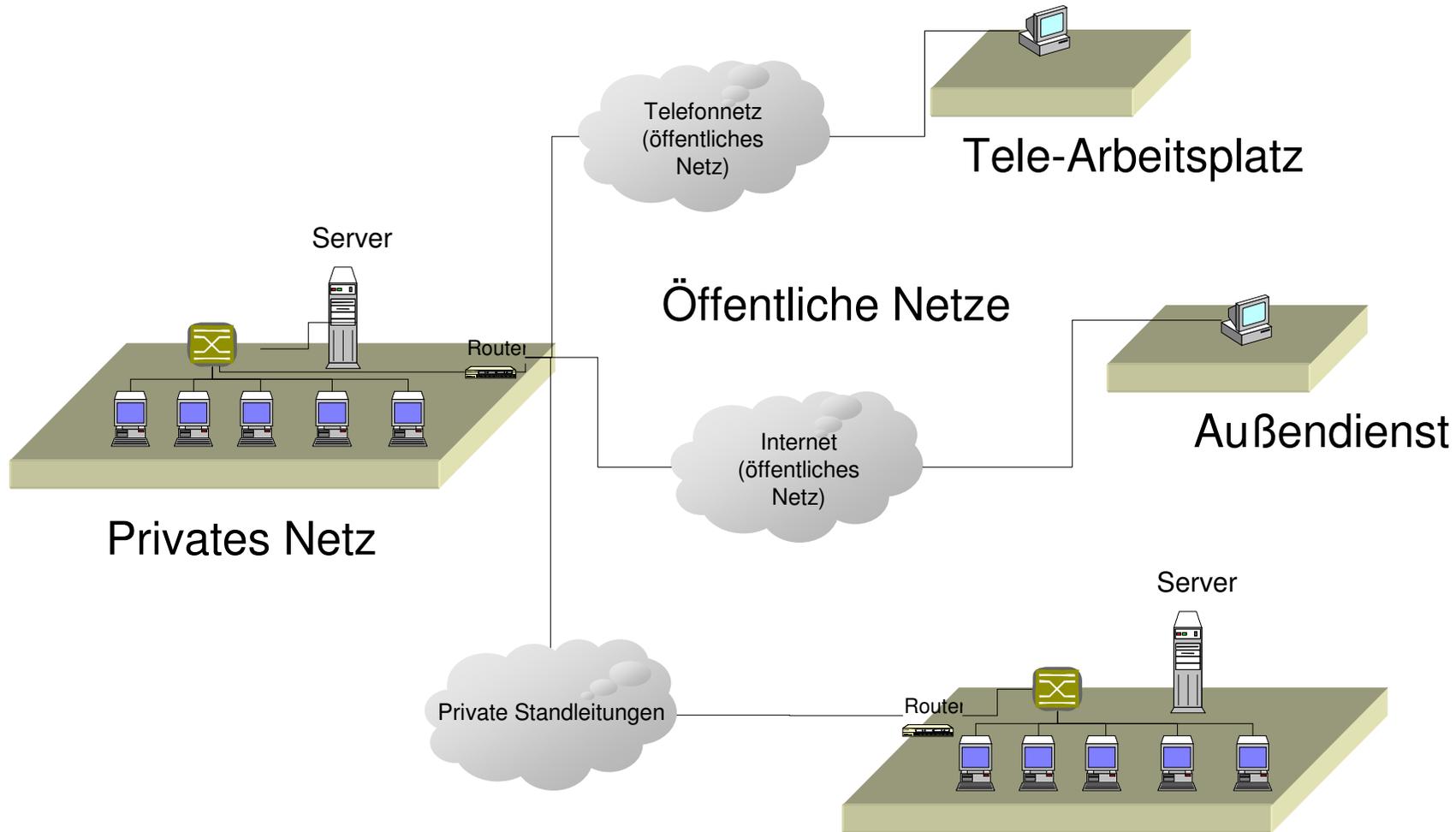
- ist Voraussetzung für eine funktionierende Informationsgesellschaft.
- trägt zur Modernisierung der Verwaltungen bei:
 - Verwaltungsprozesse müssen überarbeitet werden
 - Erreichbarkeit wird erhöht
 - Abläufe und Normen werden in Frage gestellt und
 - Prozesse werden automatisiert

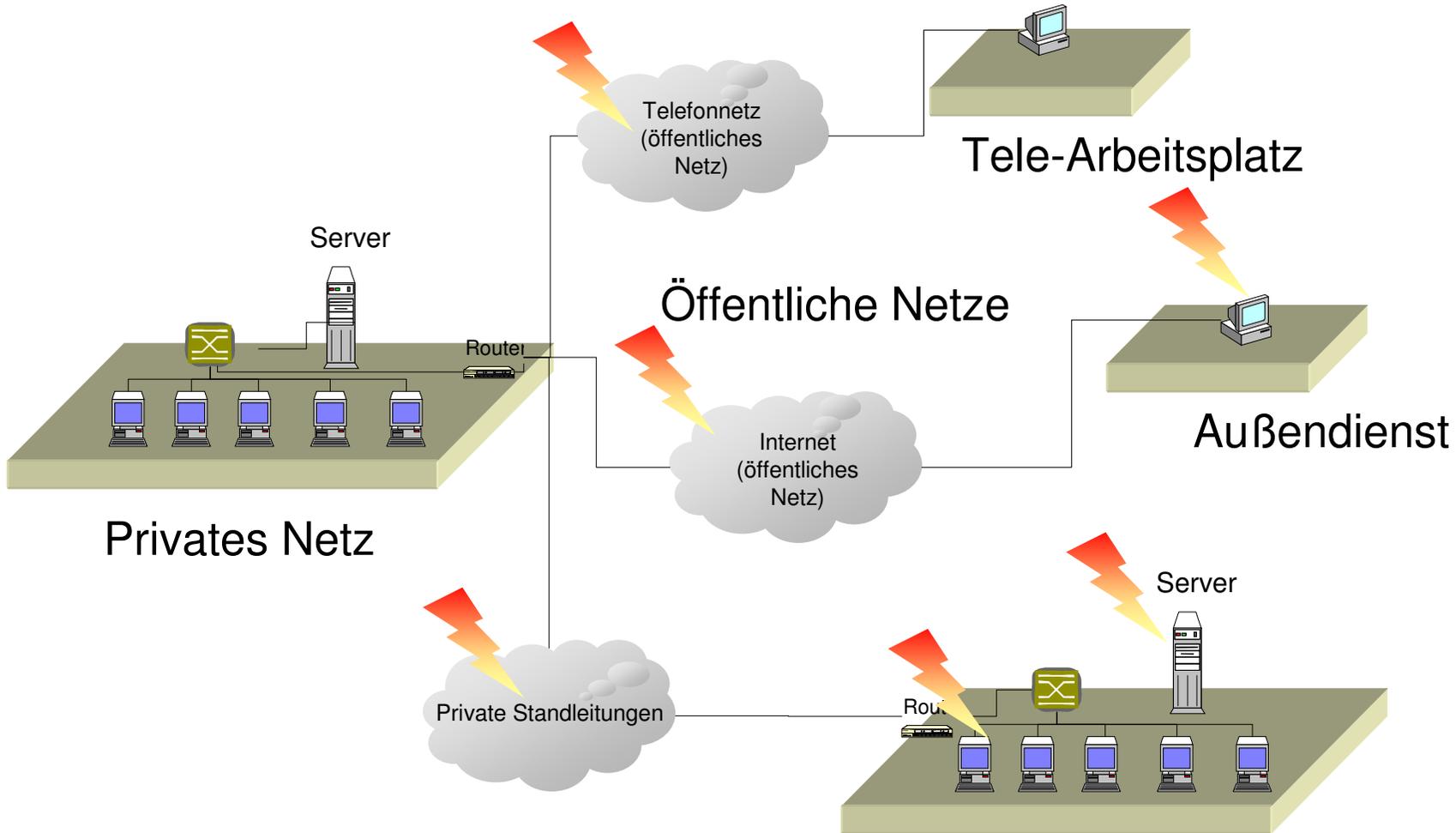
Treten Personen nur „elektronisch“ gegenüber, bedarf es funktionierender Identitätsmanagement- und Verschlüsselungslösungen, die technologisch und organisatorisch reibungslos funktionieren und effizienter als der bisherige Weg sind.

Umsetzungsstand



Realisierte Dienstleistungen	bis 2002	2002	bisher 2003	bisher insgesamt
Bereitstellung von Informationen	17	103	21	141
Beratung	0	6	0	6
Vorbereitung von politischen Entscheidungen	0	0	0	0
Zusammenarbeit mit Behörden	2	4	0	6
Antragsverfahren	1	9	4	14
Förderungen	1	1	1	3
Beschaffungsvorhaben	0	3	4	7
Durchführung von Aufsichtsmaßnahmen	0	4	3	7
Sonstige Dienstleistungen	2	15	4	21
Dienstleistungen insgesamt	23	145	37	205



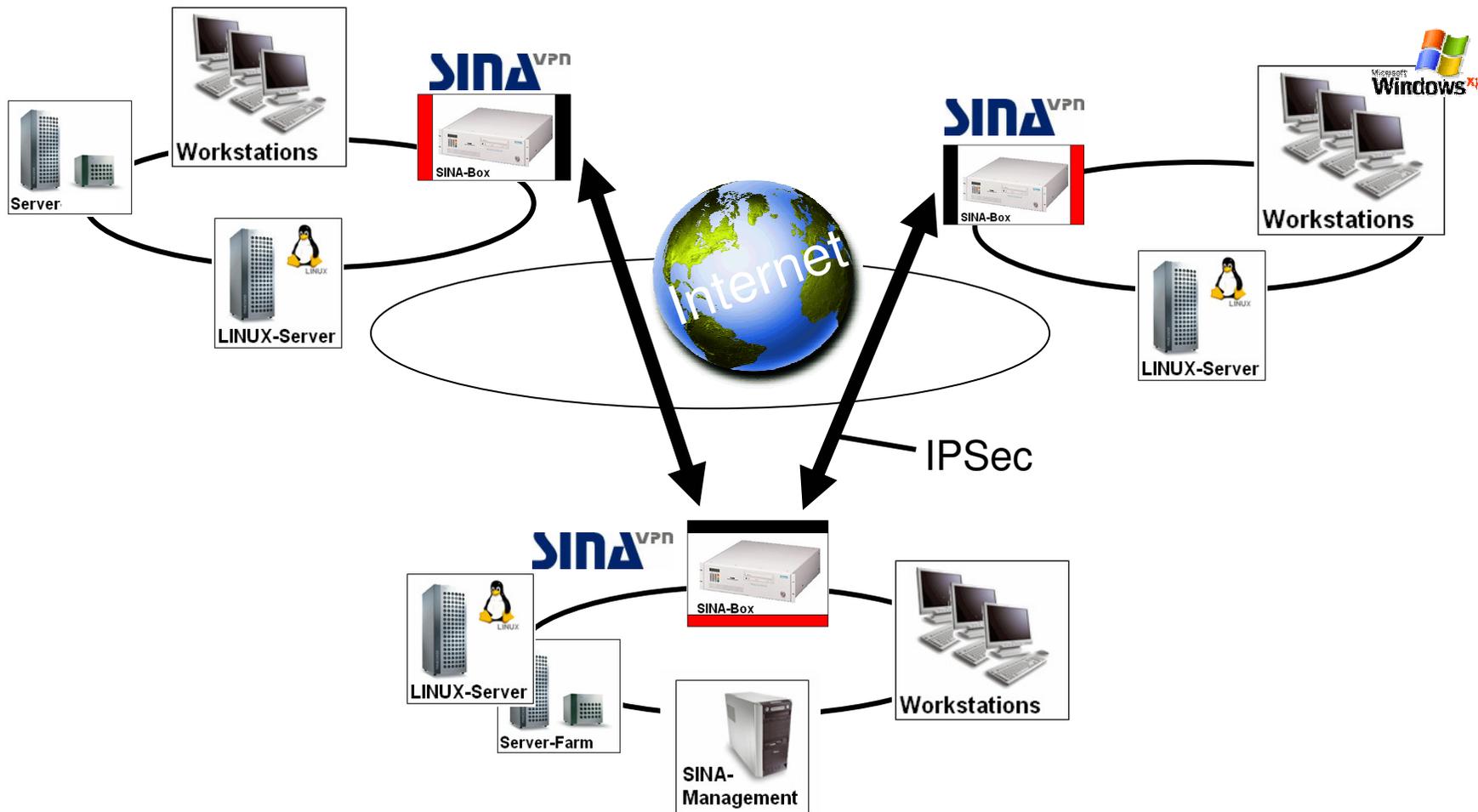


Hochsicheres smartcard gesichertes VPN

- SINA realisiert hochsichere VPNs (virtual private networks) über unsichere Netzwerke (z.B. Internet)
- gleichzeitiger Zugang zu verschiedenen klassifizierten Netzen mit einem Rechner
- Sicherheit der Client-Umgebung integriert
- flexible Architektur
 - Schicht-3-VPN
 - modularisierte Kryptoalgorithmen
 - Kombination von Thin Client / VPN / Management Komponenten
- Lösung basiert auf Open Source
- Kooperation zwischen Bundesamt für Sicherheit in der Informationstechnik (BSI) und secunet
 - Evaluation
 - Zulassung
 - Einstufung Geheim seit 02/2003



Anwendungsbeispiel VPN





2^B Advice

SINA-Komponenten

SINA Box
SINA Thin Client
SINA Management



SINA Box

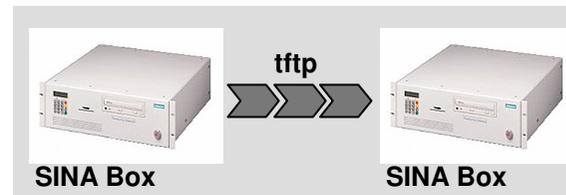


SINA Client



SINA Management

SINA One-Way Gateway



SINA Virtual Workstation
SINA Encapsulated Server

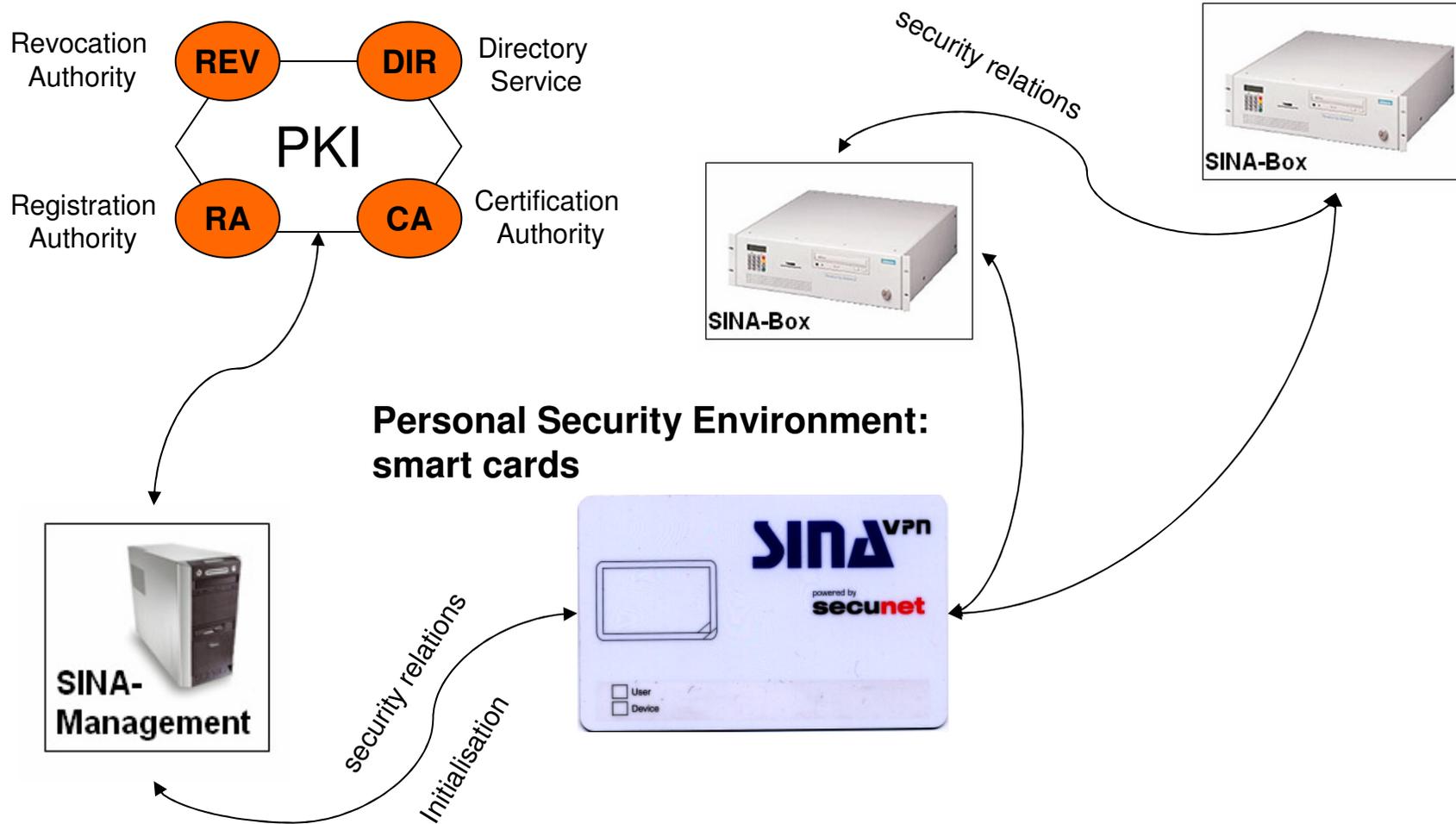


Virtual WS



Encap. -Server

Sicherheitsmanagement

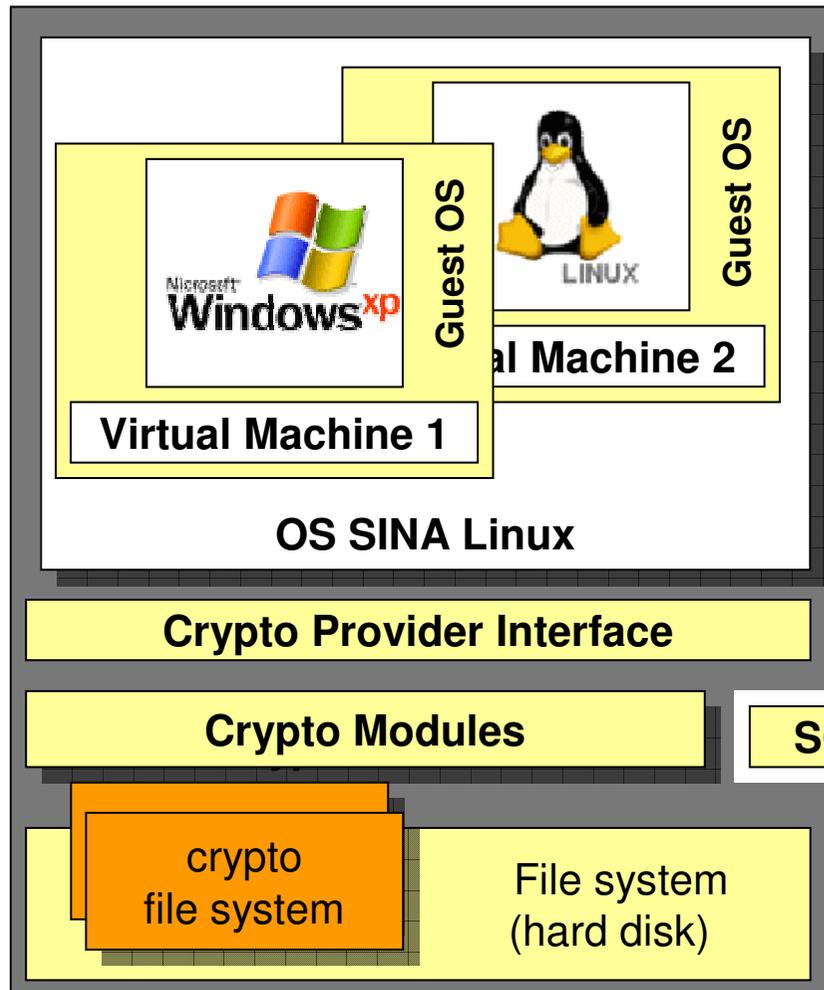


SINA - Virtual WS



operating systems (OS) are completely encapsulated by the SINA system

Virtual Machine



confidential data are kept in a crypto-file system

Virtuelle Poststelle

Rechtsverbindliches E-Government bedarf **anspruchsvoller technischorganisatorischer Voraussetzungen**, um die Integrität, Authentizität, Vertraulichkeit und Nachweisbarkeit der Kommunikation zu gewährleisten:

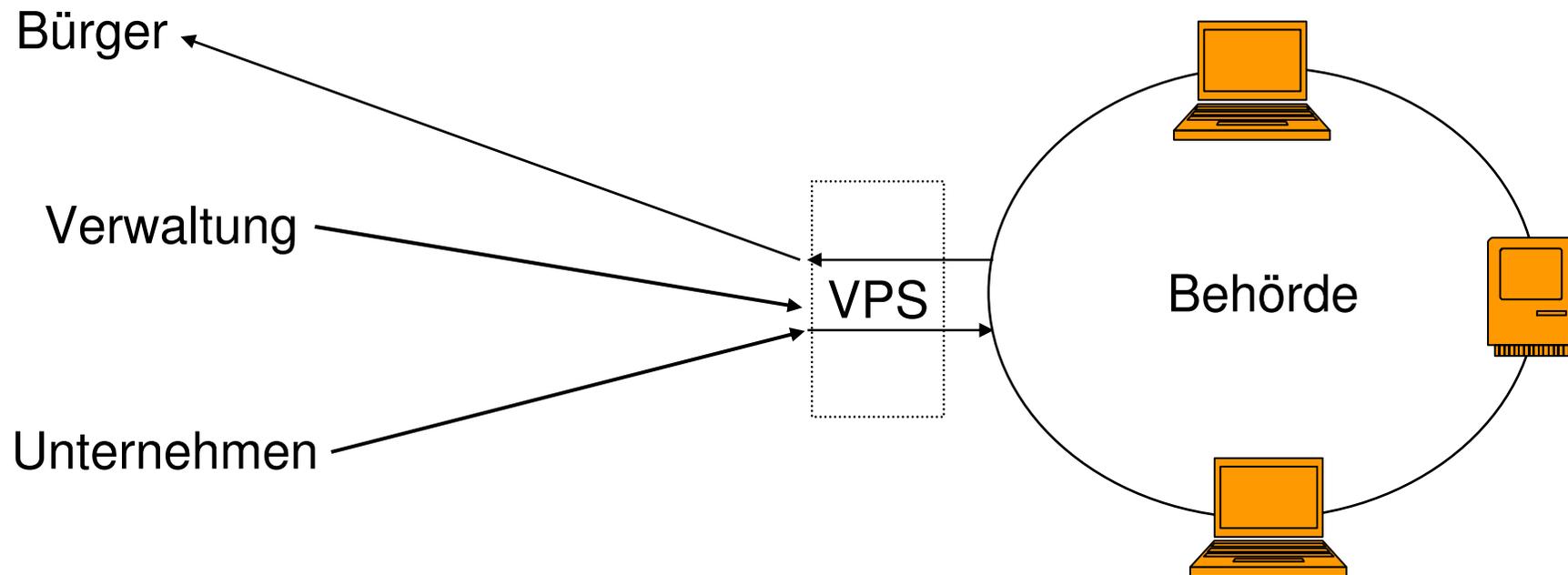
- Signaturerstellung/-prüfung
- Ver-/Entschlüsselung

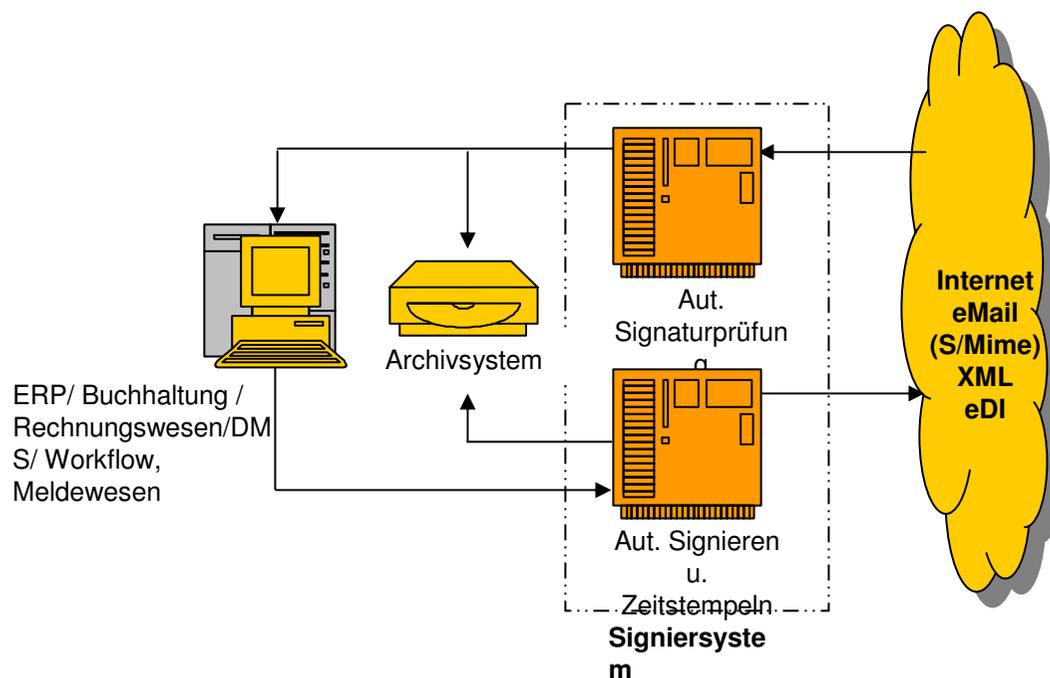
Sollen diese Voraussetzungen bei **jedem Mitarbeiter der Verwaltung** einzeln geschaffen werden, ist dies in mehrfacher Hinsicht problematisch:

- **hohe Kosten** für den Aufbau der technischen Infrastruktur an jedem Arbeitsplatz und für die Vermittlung der notwendigen Kenntnisse
- Kommunikation kann nicht auf Viren gescannt werden
- **dauerhafte zusätzliche Belastung** der Mitarbeiter

Geringer Implementierungsaufwand

Virtuelle Poststellen (VPS) sind zentrale Kommunikationsstellen, die möglichst alle erforderlichen Sicherheitsdienste bereitstellen und dadurch die Kommunikationspartner Mitarbeiter entlasten.

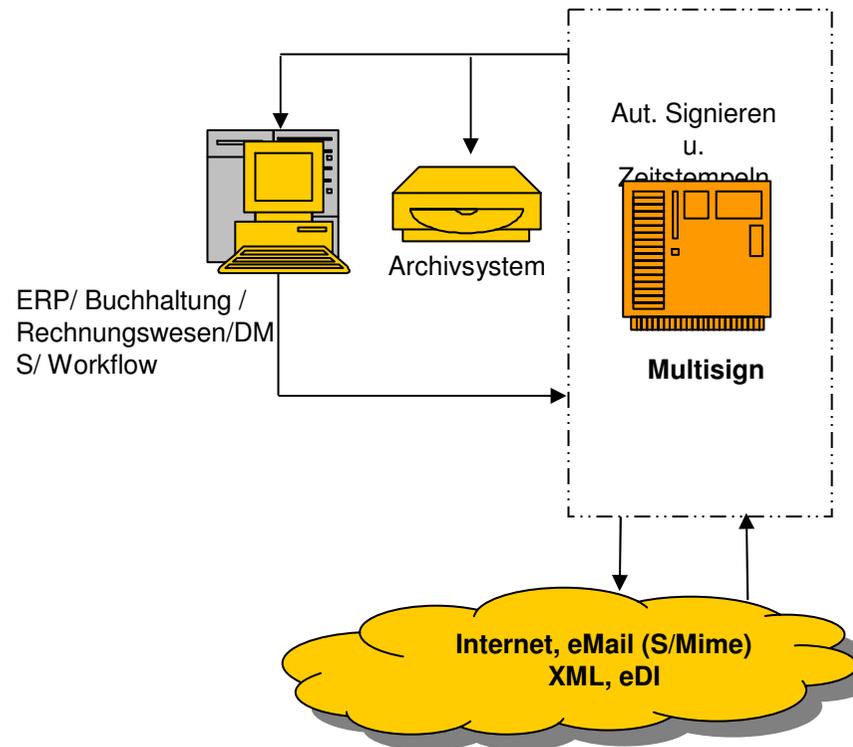




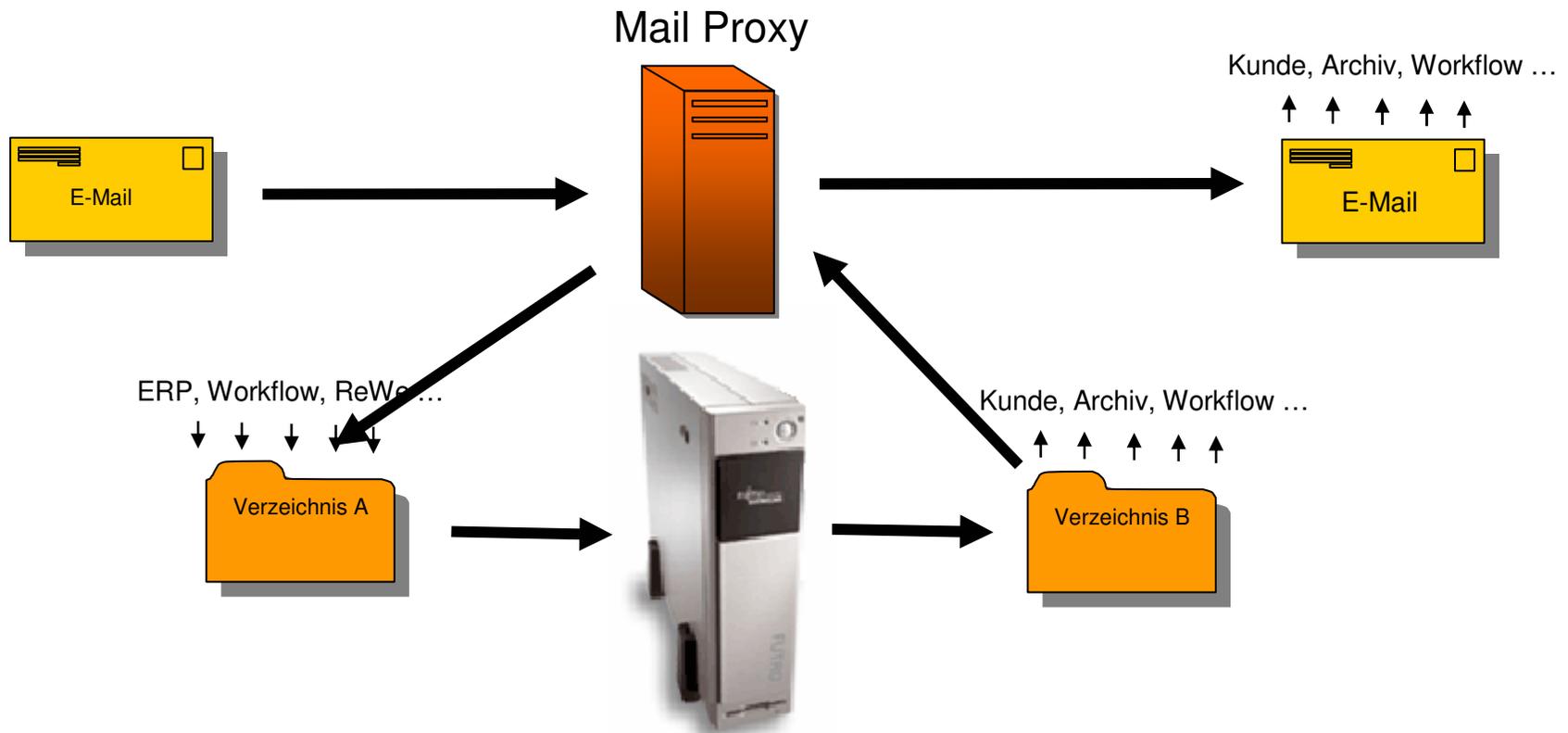
Dedizierte Signatur & Verschlüsselungsserver

- Einsatz eines oder mehrere Signaturserver
- System E2Hoch evaluiert oder Herstellererklärung
- Evtl. Mandantenfähig für verschiedene Abteilungen.
- Prüfkomponeute für Einzelprüfung
- Automatisierte Erstellung und Prüfung der Signatur
- Verschlüsselung und Entschlüsselung erfolgt analog

Funktionsweise Bsp. Signaturprozess 1/2



Funktionsweise Bsp. Signaturprozess 2/2

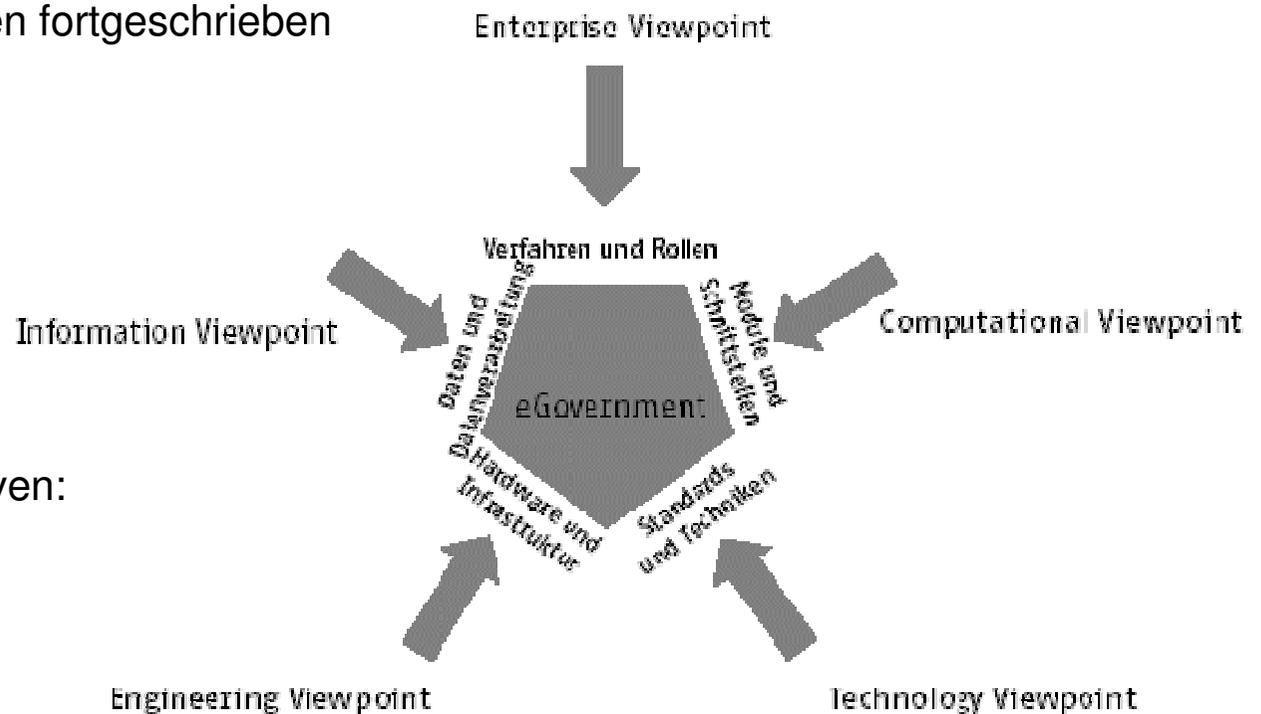


Standards 1/3: SAGA

Standards an denen im eGovernment keiner vorbeikommt:

SAGA (**S**tandards und **A**rchitekturen für **eG**overnment **A**nwendungen)

- bündelt alle obligatorischen und empfohlenen Standards
- wird in regelmäßigen Abständen fortgeschrieben
- ist normativ



Zusammenschau in 5 Perspektiven:

Standards 2/3: ISIS-MTT

ISIS-MTT

- Interoperabilitätsspezifikation
 - Profilierung international etablierter Standards
 - Interoperabilität zwischen unterschiedlichen Sicherheitsniveaus
- Umfasst
 - Spezifikationen und Testspezifikationen
Neu (ab November): XML-Signatur und Verschlüsselung
 - Testbett
frei verfügbarer Testserver
 - Konformitätssiegel
- Gemeinsame Initiative von TeleTrust und T7 (Trustcenter)
 - Gefördert vom BMWA
 - Obligatorisch in SAGA

Standards 3/3: OSCI

OSCI

- OSCI Transport
 - Grundlegendes Verfahren zur Abwicklung von eGovernment Transaktionen
 - XML-basiert (SOAP Messages)
 - XML Digitale Signatur integriert
 - Neu:** Ab November harmonisiert mit ISIS-MTT
 - Entstanden aus Media@Komm in Bremen
 - Obligatorisch in SAGA
- XMeld
 - Vereinheitlichung der Meldedatensätze
 - Beispiel: „länderübergreifende Rückmeldung“ damit möglich
 - Verankerung in den verantwortlichen Gremien (KoopA ADV)
 - Version 1.1 seit 21.07.2003

Beispiele: „Sichere eGovernment Lösungen“



- **Beschaffung durchführen**; Beschaffungsamt des Bundesministerium des Innern
Auf der Vergabepattform des Beschaffungsamtes des BMI können aktuelle Ausschreibungen eingesehen werden und eigene Angebote auf elektronischem Weg an das Beschaffungsamt übermittelt werden.
- **Virtuelles Rathaus Hagen**
- **Bremen-Online**

Kontakt



Firmensitz 2^B Advice GmbH:

Kölnstraße 103

53111 Bonn

Fon_+49 22 8 96397690

Fax_+49 22 8 96397692

Büro Dortmund / Unna:

Platanenallee 17

59425 Dortmund / Unna

Online:

Mail_ info@2b-advice.com

Web_ <http://www.2b-advice.com>