Lotus software

IBM

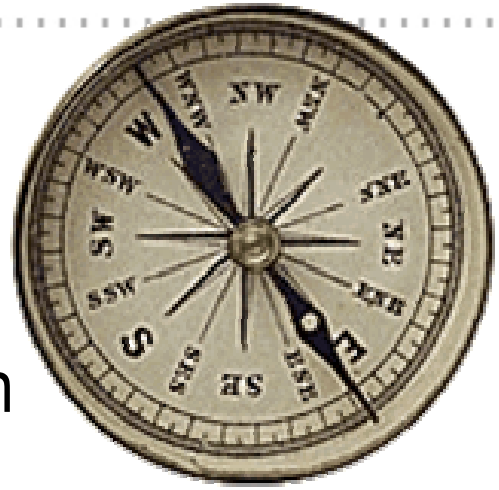
e business software

Integrierte Sicherheitslösungen auf Basis von Lotus Domino

Boris Baltzer, IBM Deutschland GmbH
boris.baltzer@de.ibm.com

IBM Software Group

360°-Sicherheit in der Kommunikation – fachliche Ziele



- Einbindung von Kunden und Bürgern in sichere Prozesse
- Einhaltung der gesetzlichen Vorschriften bei der Übertragung sensibler Daten
- Nutzung der hohen Sicherheit, die Smartcards von Trustcentern und Banken bieten
- Minimierung des Aufwandes
  - keine zusätzliche Software am Arbeitsplatz
  - keine zusätzliche Software beim Kunden

360°-Sicherheit in der Kommunikation – technische Ziele

- Authentifizierung
  - Abgestufte Sicherheit
- Signatur
  - Konform zum Signaturgesetz
- Sichere Dokumentenübertragung
  - An Benutzer mit und ohne Zertifikat
- Self-Service – nur geringe zusätzliche administrativen Aufwände

Anforderungen an die Authentifizierung

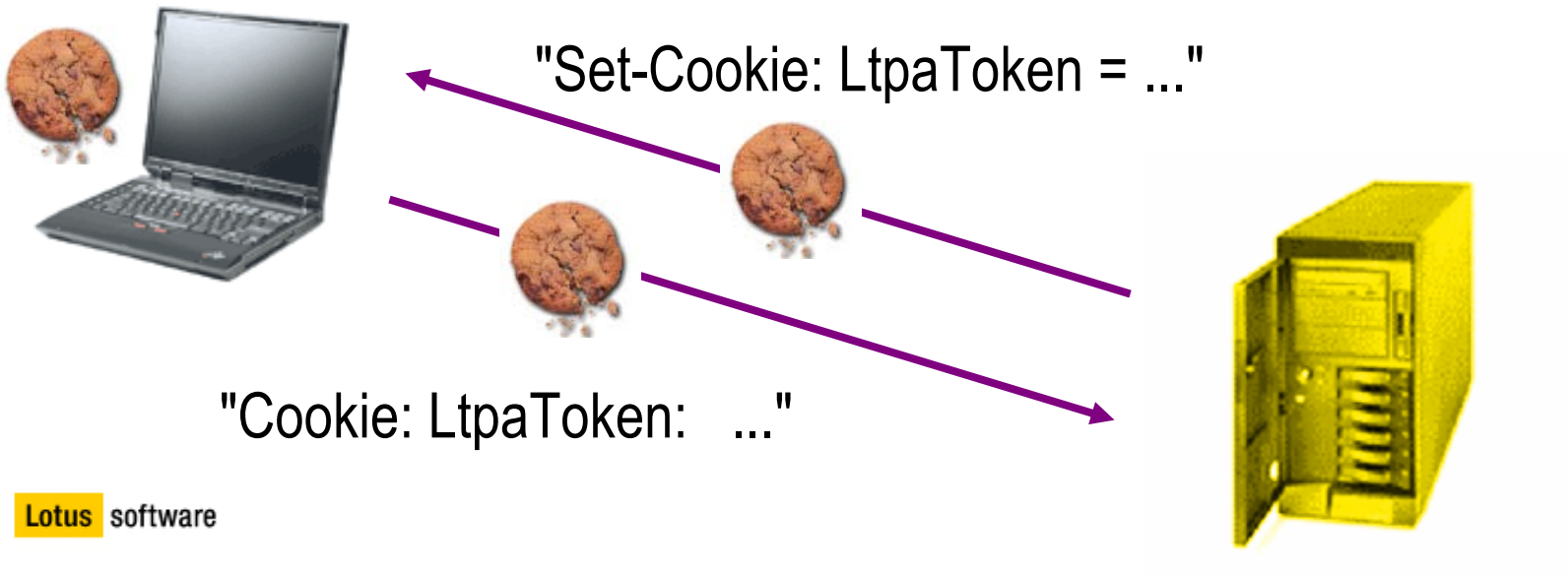
- Unterstützung von SigG-konformen SmartCards
- Zuordnung registrierte Benutzer
- Zulassung unregistrierte Benutzer
  - über definierte Zulassungsprozesse
- Keine Softwareinstallation auf dem Client
- Serverübergreifende Authentifizierung
  - Der Benutzer muss, nachdem er einmal authentifiziert wurde, innerhalb einer Anwendung und auf allen Servern stets wieder erkannt werden (Single Sign-On)

Bestehende Single Sign-On Implementierung

- Der Benutzer bekommt nach der ersten Authentifizierung ein eindeutiges Token, dass automatisch bei weiteren Seitenaufrufen übertragen wird.
  - Cookie
  - URL-Rewriting
  - Zertifikat

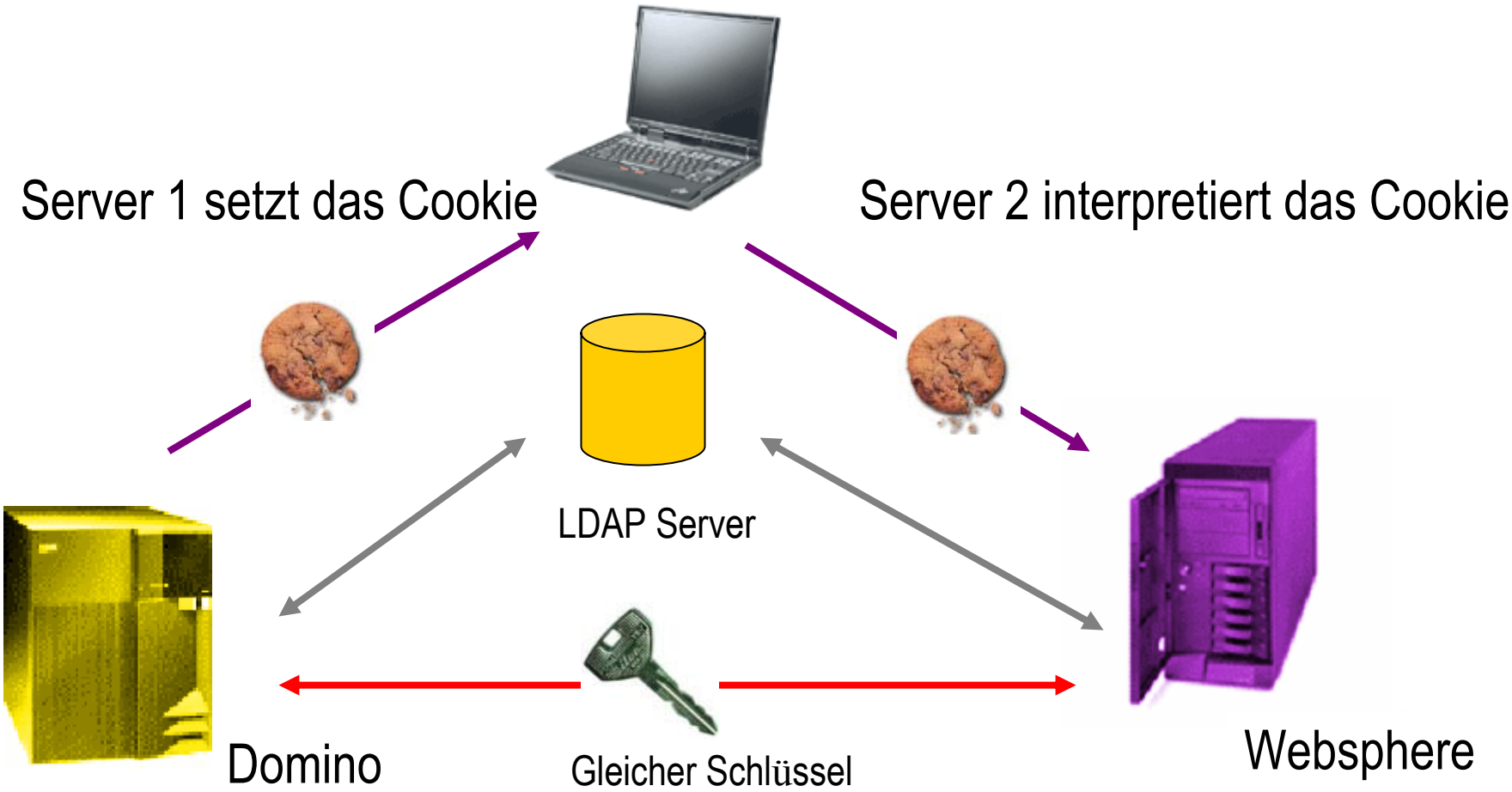
LTPA Session Authentication (WebSphere, Domino)

- So funktioniert's
  - Benutzer wird Authentifiziert
  - Der Server sendet ein Cookie an den Browser
  - Der Browser überträgt den Cookie bei weiteren Anfragen
- Inhalt des LTPA Cookie
  - Name“LtpaToken”, Domain Name, User Name (signiert und verschlüsselt) Expiration Date and Time (signiert und verschlüsselt)



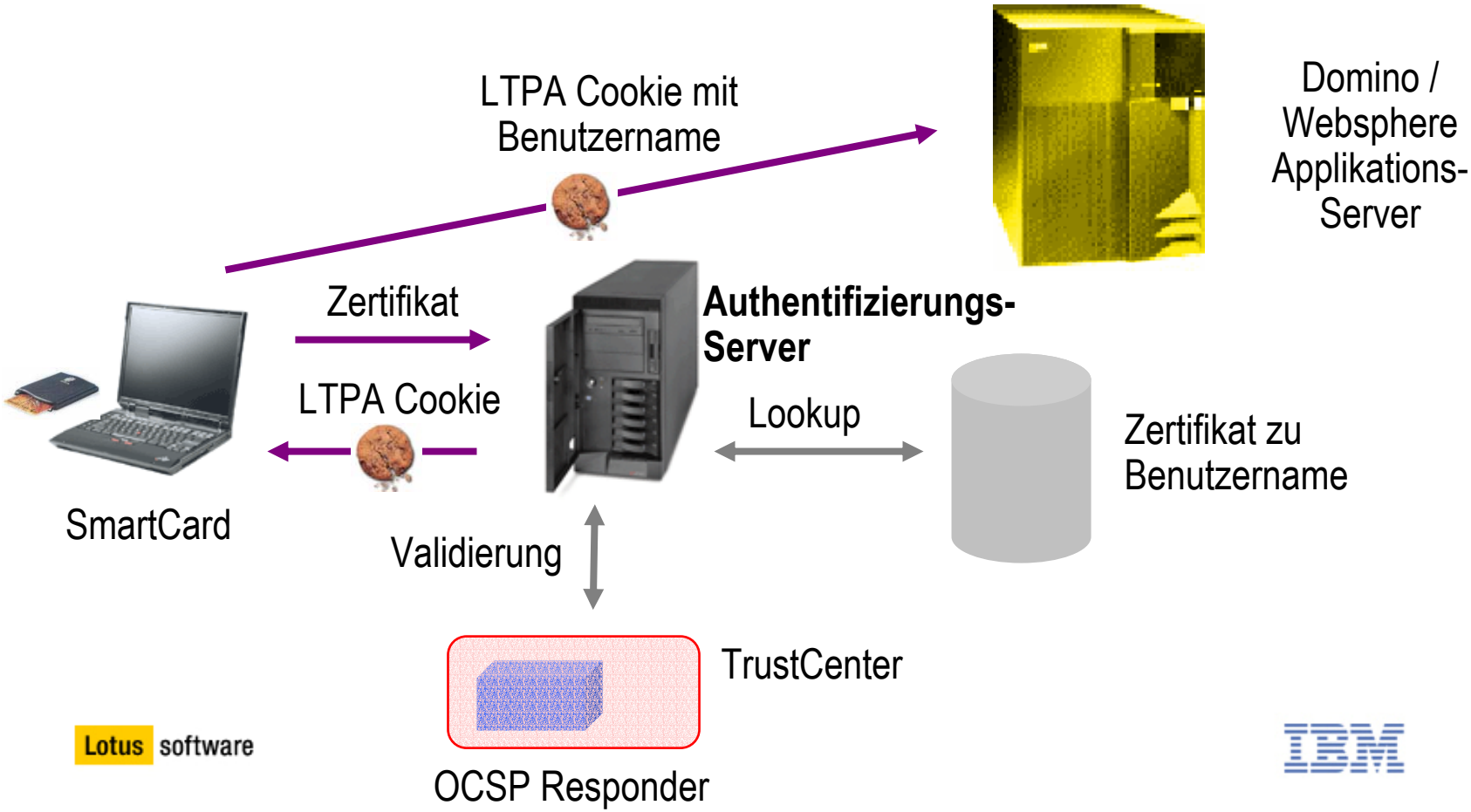
LTPA Session Authentication (mehrere Server)

- Die Server vertrauen der Unterschrift des Cookies (gleicher Schlüssel).
- Das Cookie wird benutzt, um eine domänen-weite Session zu steuern.



Authentifizierungs-Server zur Einbindung beliebiger TrustCenter

- Integration von "öffentlichen" TrustCentern
  - Kunden werden über die von Banken, TrustCentern etc. ausgegebenen SmartCards identifiziert



Lotus software

IBM

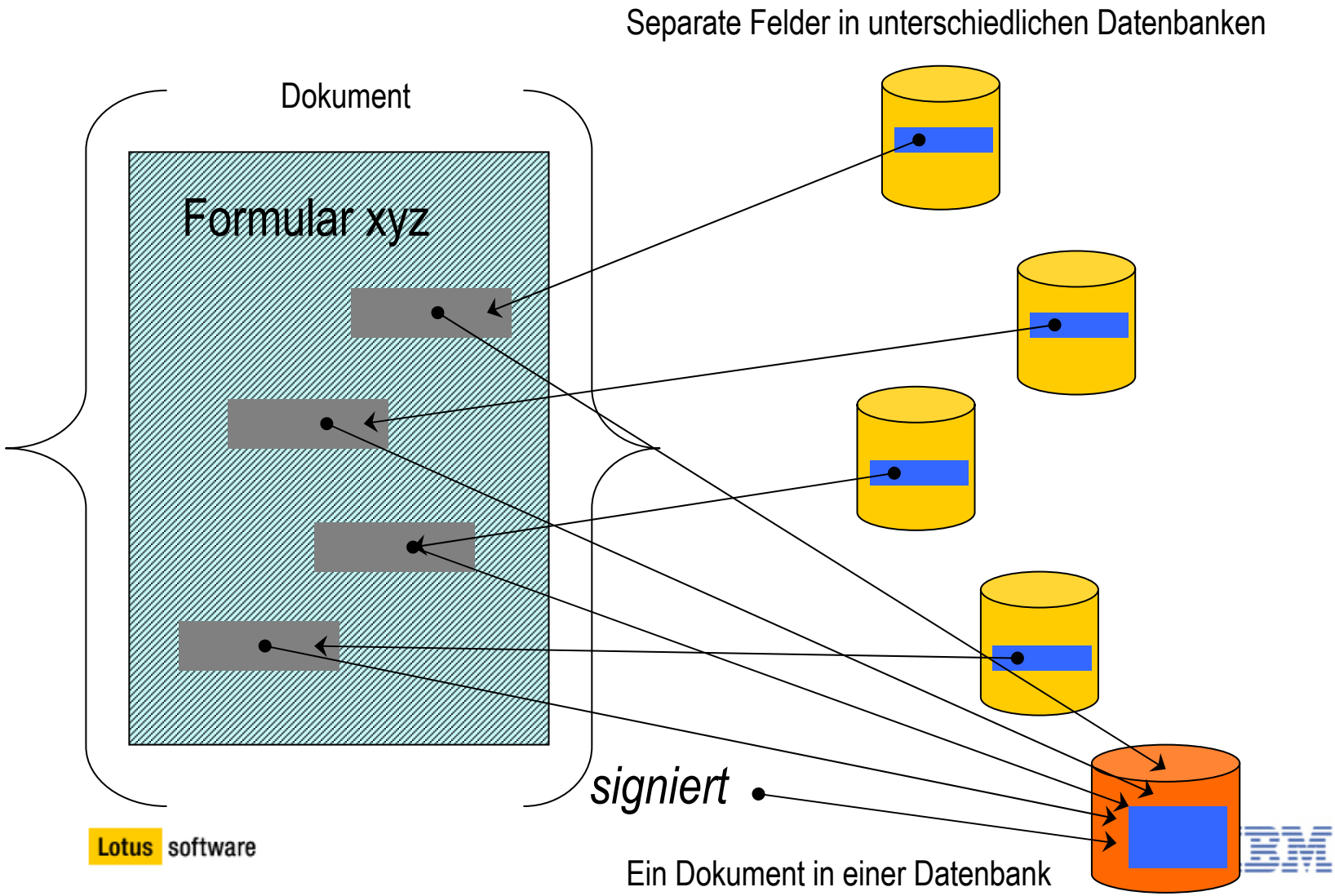
Anforderungen an die Signatur - fachlich

- SigG-Konform
- Nachvollziehbar
  - was?
  - wann?
  - von wem?
- Unterstützung der
  - Erstellung
  - Archivierung
  - Validierung

Anforderungen an die Signatur - technisch

- Einbindung in den Browser-Kontext (und ggf. Notes Kontext)
  - Verzicht auf Softwareinstallation auf dem Client
- Problemlose Weiterverarbeitung in Domino und Websphere
- Unabhängig von speziellen
  - Browsern
  - Betriebssystemen
  - Kartenlesern / Karten

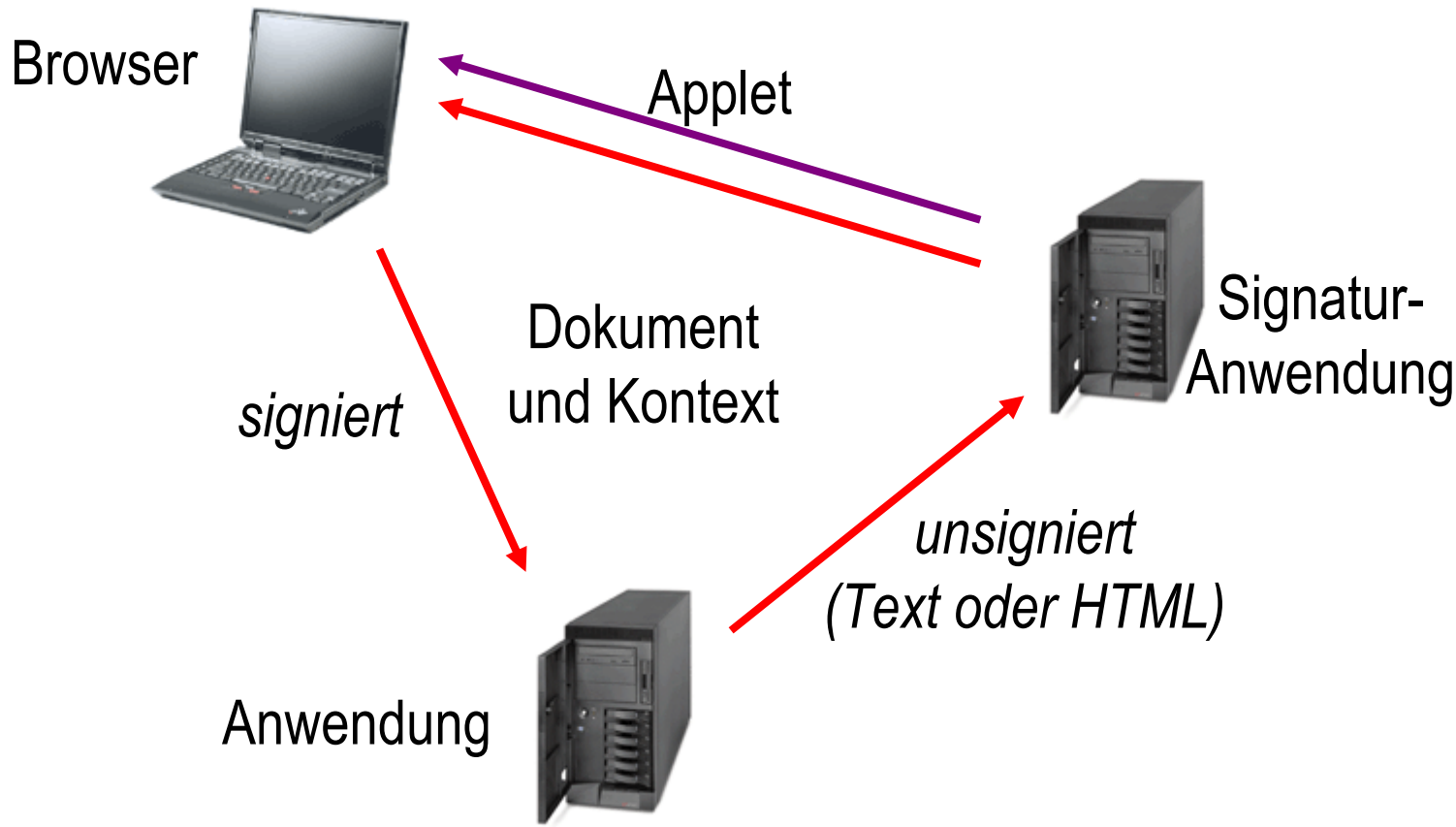
Unterschreiben in dynamischen Anwendungen



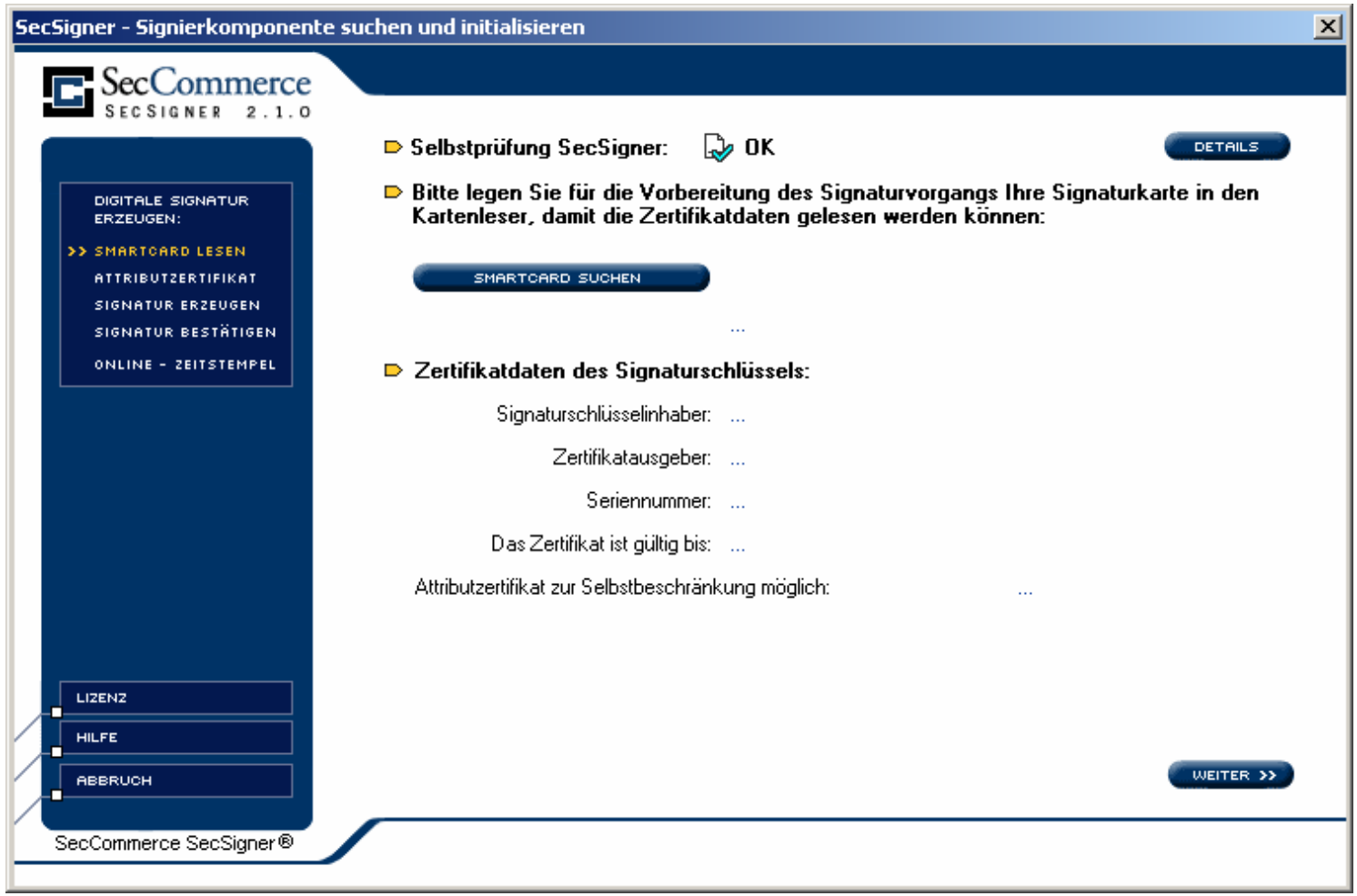
Lotus software

IBM

Ablauf der Signatur

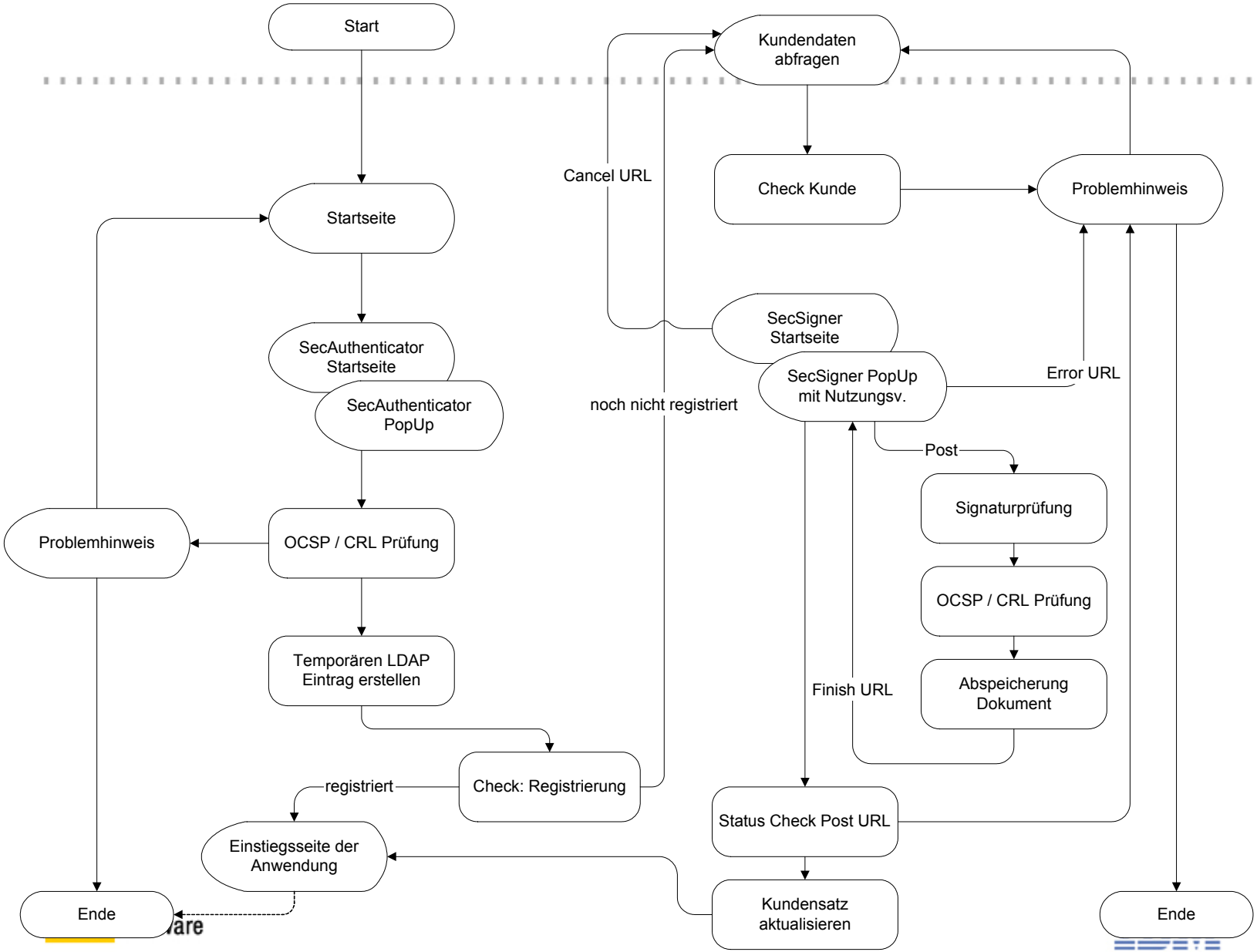


Demo



Lotus software

IBM


Start
Startseite
SecAuthenticator Startseite
SecAuthenticator PopUp
OCSP / CRL Prüfung
Problemhinweis
Temporären LDAP Eintrag erstellen
Check: Registrierung
registriert
Einstiegsseite der Anwendung
Ende
Kundendaten abfragen
Cancel URL
Check Kunde
Problemhinweis
SecSigner Startseite
noch nicht registriert
SecSigner PopUp mit Nutzungsv.
Error URL
Post
Signaturprüfung
OCSP / CRL Prüfung
Abspeicherung Dokument
Finish URL
Status Check Post URL
Kundensatz aktualisieren
Ende

Anforderung an die sichere Übertragung von Dokumenten

- Flexible Adaption an bestehende Systeme
- Geringer Wartungsaufwand
- Hohe Akzeptanz bei Kunden und Mitarbeitern
- Nachweislich hohe Sicherheit
- Standardkonformität
  - SPHINX
  - S/MIME Implementierung in Standardprodukten
  - Bridge CA

Alternativen der sicheren Dokumentenübertragung

- Verschlüsselung des Dokumentes (S/MIME)
  - „Ende zu Ende“ Verschlüsselung (Verschlüsselung am Arbeitsplatz)
  - Zentrale Verschlüsselung durch ein Gateway
- Verschlüsselung der Verbindung (SSL)
  - Bereitstellung eines Dokumenten-Servers und Etablierung eines sicheren Zuganges

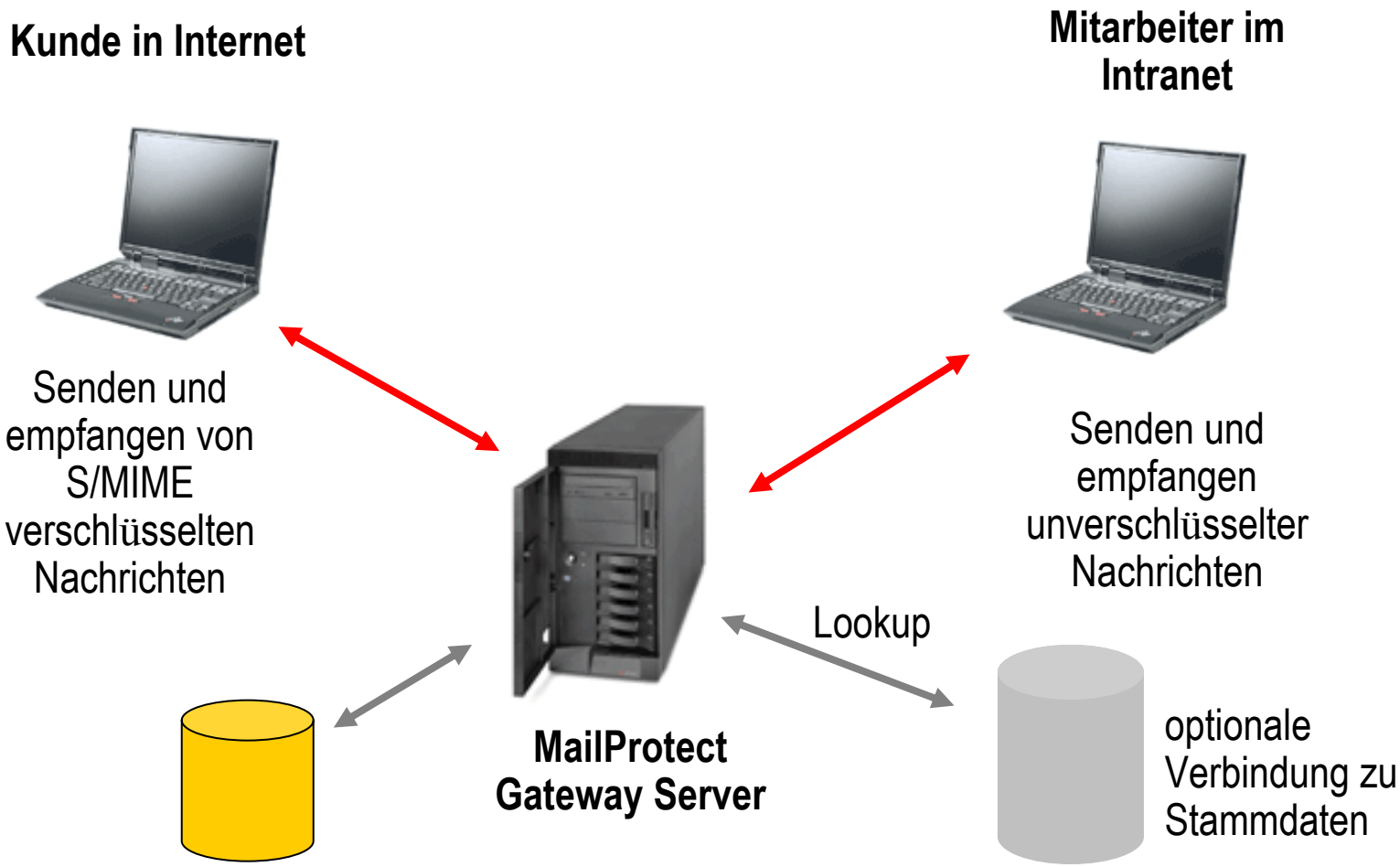
„Ende zu Ende“-Verschlüsselung

- Vorteile
  - Die Nachricht ist auf der gesamten Übertragungsstrecke verschlüsselt
  - Standardisierung der Clients durch das BSI im Rahmen des SPHINX Projektes
- Nachteile
  - Die Verschlüsselung ist personenbezogen und unterstützt keine Gruppenpostkörbe
  - Zentrales Virenscannen ist unmöglich
  - Vertretungsregelungen können nicht implementiert werden
  - Benutzer werden mit allen Zertifikat bezogenen Problemen direkt konfrontiert
  - Die Verteilung und Verwaltung der Zertifikate ist sehr aufwendig

Zentrale Ver- und Entschlüsselung mit MailProtect Gateway

- E-Mail wird beim Durchlaufen eines zentralen Gateways verschlüsselt, entschlüsselt, signiert oder validiert
- Das Verfahren ist auch auf Gruppenpostkörbe anwendbar
- Zentrales Virenscannen ist kein Problem
- Unabhängigkeit von Client (auch für iNotes Web Access, Web-Mail, Host-Systeme geeignet)
- Keine Softwareinstallation auf dem Client
- Das Handling der Zertifikate kann zentral organisiert werden

Einbindung von MailProtect Gateway



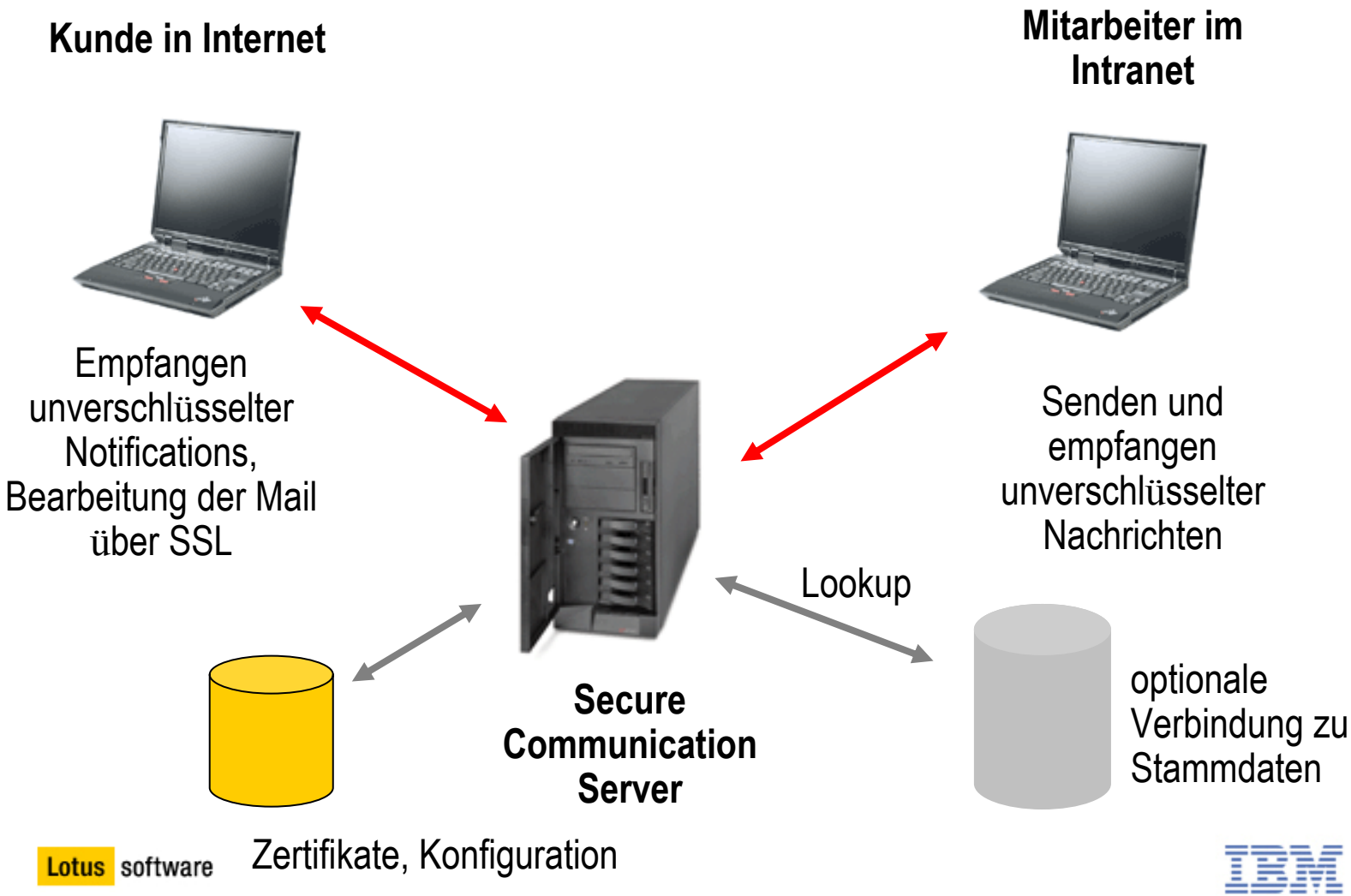
Lotus software

IBM

Verschlüsselung durch den Secure Communication Server (SCS)

- Für jeden Kunden werden die E-Mails auf dem SCS verwaltet
- Der Zugriff erfolgt Passwort oder Zertifikat gesichert über eine SSL-Verbindung
- Der Kunde wird benachrichtigt, wenn neue Informationen für ihn vorliegen
- E-Mails und Formulare können problemlos kombiniert werden
- Backend-Daten lassen sich einfach integrieren
- Der Kunde verwaltet seine Daten weitgehend selbst

Einbindung des Secure Communication Servers



Lotus software

IBM

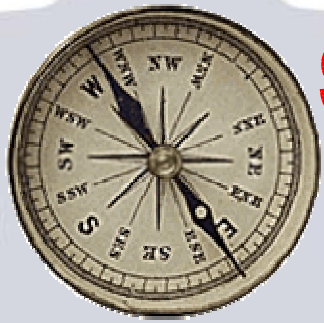
360°-Sicherheit in der Kommunikation

Ihre Fragen

Kunden - Mitarbeiter - Legacy Systems - Partner

Authentication

SSL



S/MIME

SmartCard

SigG