Lars Pickel

Planung einer Public-Key-Infrastruktur und Pilotierung für die E-Mail-Kommunikation

Diplomarbeit

Diplom.de

Bibliografische Information der Deutschen Nationalbibliothek:

Bibliografische Information der Deutschen Nationalbibliothek: Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de/ abrufbar.

ISBN: 9783832427306

Lars Pickel

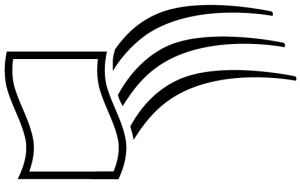
Planung einer Public-Key-Infrastruktur und Pilotierung für die E-Mail-Kommunikation

Diplom.de

Lars Pickel

Planung einer Public-Key-Infrastruktur und Pilotierung für die E-Mail-Kommunikation

Diplomarbeit
an der Fachhochschule Wiesbaden
Fachbereich Informatik
Juli 2000 Abgabe



***Diplomarbeiten* Agentur**
Dipl. Kfm. Dipl. Hdl. Björn Bedey
Dipl. Wi.-Ing. Martin Haschke
und Guido Meyer GbR

Hermannstal 119 k
22119 Hamburg

agentur@diplom.de
www.diplom.de

ID 2730

ID 2730
Pickel, Lars: Planung einer Public-Key-Infrastruktur und Pilotierung für die E-Mail-Kommunikation / Lars Pickel -
Hamburg: Diplomarbeiten Agentur, 2000
Zugl.: Wiesbaden, Fachhochschule, Diplom, 2000

Dipl. Kfm. Dipl. Hdl. Björn Bedey, Dipl. Wi.-Ing. Martin Haschke & Guido Meyer GbR
Diplomarbeiten Agentur, http://www.diplom.de, Hamburg 2000
Printed in Germany

Diplomarbeiten Agentur

Wissensquellen gewinnbringend nutzen

Qualität, Praxisrelevanz und Aktualität zeichnen unsere Studien aus. Wir bieten Ihnen im Auftrag unserer Autorinnen und Autoren Wirtschaftsstudien und wissenschaftliche Abschlussarbeiten – Dissertationen, Diplomarbeiten, Magisterarbeiten, Staatsexamensarbeiten und Studienarbeiten zum Kauf. Sie wurden an deutschen Universitäten, Fachhochschulen, Akademien oder vergleichbaren Institutionen der Europäischen Union geschrieben. Der Notendurchschnitt liegt bei 1,5.

Wettbewerbsvorteile verschaffen – Vergleichen Sie den Preis unserer Studien mit den Honoraren externer Berater. Um dieses Wissen selbst zusammenzutragen, müssten Sie viel Zeit und Geld aufbringen.

http://www.diplom.de bietet Ihnen unser vollständiges Lieferprogramm mit mehreren tausend Studien im Internet. Neben dem Online-Katalog und der Online-Suchmaschine für Ihre Recherche steht Ihnen auch eine Online-Bestellfunktion zur Verfügung. Inhaltliche Zusammenfassungen und Inhaltsverzeichnisse zu jeder Studie sind im Internet einsehbar.

Individueller Service – Gerne senden wir Ihnen auch unseren Papierkatalog zu. Bitte fordern Sie Ihr individuelles Exemplar bei uns an. Für Fragen, Anregungen und individuelle Anfragen stehen wir Ihnen gerne zur Verfügung. Wir freuen uns auf eine gute Zusammenarbeit

Ihr Team der *Diplomarbeiten* Agentur

Dipl. Kfm. Dipl. Hdl. Björn Bedey
Dipl. Wi.-Ing. Martin Haschke
und Guido Meyer GbR

Hermannstal 119 k
22119 Hamburg

Fon: 040 / 655 99 20
Fax: 040 / 655 99 222

agentur@diplom.de
www.diplom.de

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

BeurkG	Beurkundungsgesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certificate Authority (Zertifizierungsstelle)
CMS	Card Management System
CP	Certification Policy
CRL	Certificate Revocation List
DEA	Data Encryption Algorithm
DES	Data Encryption Standard
DN	Distinguished Name
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
EEPROM	Electrical Erasable Programmable Read Only Memory
EU	Europäische Union
EU-R	EU-Richtlinie
ID	Identification
IDEA	International Data Encryption Algorithm
IETF	Internet Engineering Task Force
IP	Internet Protokoll
IPX	Internet Package Exchange
ISO	International Standard Organisation
IT	Informationstechnologie
ITSEC	Information Technology Security Evaluation Criteria
ITU	International Telecommunication Union (früher CCITT)
IuKDG	Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste
LDAP	Lightweight Directory Access Protocol
MD	Message Digest
MD3	Message Digest Version 3
MD4	Message Digest Version 4
MD5	Message Digest Version 5

MEZ	Mitteleuropäische Zeit
MIME	Multipurpose Internet Mail Extensions
MTT	MailTrusT
NIST	National Institute of Standards and Technology (USA)
NSA	National Security Agency
PC	Personal Computer
PC/SC	Personal Computer/Smart Card
PEM	Privacy Enhanced Mail
PGP	Pretty Good Privacy
PIN	Personal Identification Number
PK	Public Key
PKA	Public Key Algorithm
PKCS	Public Key Cryptographic Standard
PKI	Public Key Infrastruktur
PKIX	Internet X.509 Public Key Infrastructure
PSE	Personal Security Environment
RA	Registration Authority
RAM	Random Access Memory
RegTP	Regulierungsbehörde für Telekommunikation und Post
RFC	Request For Comments
ROM	Read Only Memory
Root CA	Root Certification Authority
RSA	Verschlüsselungsverfahren benannt nach Rivest, Shamir und Adleman
S/MIME	Secure Multipurpose Internet Mail Extensions
SA	Systemadministrator
SC	Smartcard
SHA	Secure Hash Algorithm
SHS-1	Secure Hash Standard
SigG	Gesetz zur digitalen Signatur
SigV	Verordnung zur digitalen Signatur
SIM	Subscriber Identification Module
SMTP	Simple Mail Transfer Protocol

SPX	Sequence Package Exchange
SSL	Secure Socket Layer
SuV	Signatur und Verschlüsselung
TCP/IP	Transmission Control Protocol/Internet Protocol
TÜV	Technischer Überwachungsverein
VPN	Virtual Private Network
X.509	Standard for Certificates
ZPO	Zivilprozessordnung

1. Einleitung

Traditionell erfolgte der Austausch von Informationen bislang durch persönliche Treffen, mittels Post oder Telefon. Heute ist er auf vielfältigen Wegen möglich. Im Geschäfts- und Privatleben wird heutzutage immer mehr das Internet als modernes Kommunikationsmittel eingesetzt. Selbst Transaktionen, die noch vor wenigen Jahren nicht denkbar waren, wie z.B. der Abschluss von Verträgen oder die Bestellung und Bezahlung von Waren, werden mittlerweile über das Internet durchgeführt. Das veränderte Kommunikationsverhalten und das fehlende Vertrauen in offene Netze, welches bei Transaktionen mit sensiblen Daten vor allem daher rührt, dass es viel mehr Möglichkeiten gibt, die Daten unbemerkt zu manipulieren und auszuspähen als bei der herkömmlichen Übermittlung, führen zu gestiegenen Anforderungen an die Sicherheit der Kommunikation:

- Bestimmte Informationen, etwa personenbezogene Daten, müssen besonders vor unbefugtem Zugang geschützt werden. Das Mitlesen dieser Informationen bei der Übermittlung muss verhindert werden (Vertraulichkeit der übertragenen Daten).

- Übertragene Daten müssen vor Manipulation geschützt sein. Sofern dies nicht hinreichend sichergestellt werden kann, muss der Empfänger zumindest die Sicherheit haben, dass Nachrichten nicht unbemerkt verändert werden können (Integrität der Daten).

- Die Kommunikationsteilnehmer möchten einen verlässlichen Nachweis darüber, dass die Person, mit der sie kommunizieren, auch die ist, für die sie sich ausgibt (Authentizität). Dies ist die wesentliche Voraussetzung für das Zustandekommen vertrauensbasierter Geschäftskontakte zum Beispiel bei Vertragsabschlüssen.

- Besonders im Geschäftsverkehr kann es für den Absender einer Nachricht wichtig sein, nachweisen zu können, dass er seine Mitteilung zu einem

bestimmten Zeitpunkt tatsächlich abgeschickt hat, z.B. wenn es um die Einhaltung von Fristen geht (Nichtabstreitbarkeit des Datenaustausches).

Um diesen Ansprüchen an eine sichere Kommunikation gerecht zu werden, wurden verschiedene Sicherheitstechnologien entwickelt, die mit der Einführung von Sicherheitsstrukturen kombiniert werden. Grundlage dieser Technologien ist die Kryptographie, die die Vertraulichkeit von Nachrichten garantiert, sowie darauf aufbauend die digitale Signatur, die für die Authentizität des Kommunikationspartners und die Integrität der Daten sorgt und somit die Voraussetzungen für die Verbindlichkeit der elektronischen Kommunikation schafft. Der Einsatz dieser Technologien basiert auf der sicheren Zuordnung eines Schlüssels zu einer Person im Rahmen einer Public-Key-Infrastrukur, welche die Gesamtheit aller technisch und organisatorisch zu leistenden Anforderungen beinhaltet.

Gegenstand dieser Arbeit ist es, am Beispiel der Sema Group CGTec GmbH den Aufbau einer Public-Key-Infrastruktur zu planen, die die technischen und organisatorischen Voraussetzungen für eine gesicherte elektronische Kommunikation unter Einbeziehung von Sicherheitshierarchien schafft, sowie deren Implementierung in einem Pilotprojekt.

2. Kryptographie: Datensicherheit in offenen Umgebungen

Das Versenden von Briefen und Dokumenten auf herkömmlichem Weg geschieht in der Regel in einem geschlossenen Umschlag. Der Grund ist einleuchtend: die Mitteilung ist ausschließlich für den Empfänger bestimmt und da am Transport dieser Informationen zahlreiche Personen beteiligt sind, ist es selbstverständlich, die Nachricht vor Einsichtnahme durch Unbefugte zu schützen. Dennoch gibt es eine nicht zu unterschätzende Anzahl von Kommunikationsteilnehmern, die beim Übermitteln von Daten den elektronischen Weg nutzen, ohne sich Gedanken über die Wahrung ihrer Privatsphäre zu machen. Ein Datenaustausch per Email erfolgt im Gegensatz zum Versenden von Dokumenten per Post nicht in einem „geschlossenen Umschlag“ sondern ähnlich wie bei einer Postkarte. Die Email passiert während ihrer Übertragung vom Sender zum Empfänger zahlreiche Stationen, bei denen die Möglichkeit besteht, dass ein Dritter die Nachricht mitliest. Um dies zu verhindern, setzt man in zunehmendem Maße Verfahren ein, die es dem Teilnehmer ermöglichen, eine Datei zu verschlüsseln.

2.1 Symmetrisches Verschlüsselungsverfahren

Beim symmetrischen Verschlüsselungsverfahren tauschen die Kommunikations-partner zunächst über einen sicheren Kanal (auf postalischem Weg oder persönlich) einen Schlüssel aus (siehe Abbildung 1 Punkt ①), den sowohl der Sender zum Verschlüsseln als auch der Empfänger zum Entschlüsseln der zu übermittelnden Nachricht verwenden wollen.