Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Signatur, Zertifikate und PKI

- Vorlesung Cyber-Sicherheit -

Prof. Dr. (TU NN)
Norbert Pohlmann

Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen
http://www.internet-sicherheit.de

Signatur, Zertifikate und PKI
→ Inhalt

- Ziele und Ergebnisse der Vorlesung
- Digitale Signaturen und Zertifikate
- Public-Key-Infrastrukturen
- Gesetzlicher Hintergrund
- PKI-enabled Application
- Zusammenfassung

Signatur, Zertifikate und PKI
→ Inhalt

- **Ziele und Ergebnisse der Vorlesung**
- Digitale Signaturen und Zertifikate
- Public-Key-Infrastrukturen
- Gesetzlicher Hintergrund
- PKI-enabled Application
- Zusammenfassung

Ziele und Ergebnisse der Vorlesung
→ Signatur, Zertifikate und PKI

- Gutes Verständnis für die Cyber-Sicherheitsprinzipien und Cyber-Sicherheitsmechanismen: **Digitale Signatur** und **elektronische Zertifikate**.

- Erlangen der Kenntnisse über **Public-Key-Infrastrukturen (PKI)** und **Vertrauensmodelle**.

- Gewinnen von praktischen Erfahrungen durch die Betrachtung von Beispielen zu **PKI-enabled Application**.

Signatur, Zertifikate und PKI
→ Inhalt

- Ziele und Ergebnisse der Vorlesung
- **Digitale Signaturen und Zertifikate**
- Public-Key-Infrastrukturen
- Gesetzlicher Hintergrund
- PKI-enabled Application
- Zusammenfassung

Digitale Signaturen und Zertifikate
→ Eigenhändige Unterschrift (1/2)

- Fragen, die bei einer eigenhändigen Unterschrift gestellt werden, sind:
  - Welchen Wert hat eine eigenhändige Unterschrift?
  - Wer hat etwas davon?
  - Welche Bedeutung hat die eigenhändige Unterschrift?
  - Welche Bedingungen müssen erfüllt sein, damit die Unterschrift einen Vorteil hat?

Dr. Gerd Müller
Sonnenallee 100a
1000 Wohlfühlstadt

02.01.2018

Fachgroßhandel für Waschmaschinen
Aachener Str. 70
50674 Köln

Sehr geehrter Herr Maier,

hiermit bestelle ich, auf der Grundlage Ihres Angebotes (Nr.345/11/17) vom 13.11.2017, bei Ihnen eine Waschmaschine im Wert von 650 Euro.

Mit freundlichen Grüßen

G. Müller

Gerd Müller

Digitale Signaturen und Zertifikate
→ Eigenhändige Unterschrift (2/2)

- Funktionen einer eigenhändigen Unterschrift:
  - **Abschlussfunktion**
    Vollendung einer Erklärung - hebt sich vom Entwurf ab
  - **Identitätsfunktion**
    Unterschrift macht die Identität des Ausstellers kenntlich
  - **Echtheitsfunktion**
    Dokument stammt vom Aussteller
  - **Warnfunktion**
    Schutz des Unterzeichners vor Übereilung
  - **Beweisfunktion (Urkundenbeweis)**
    Erleichtert die Beweisführung im Streitfall

Digitale Signaturen und Zertifikate
→ Digitale Signatur (1/3)

- Signaturerstellung zu einer Nachricht m:

s = S (m, GSA)

S: Signaturfunktion, z.B. RSA-Verfahren
m: Nachricht, die signiert werden soll
s: Signatur, z.B. 3.000 Bit Zeichenkette
GSA: geheimer Schlüssel des Nutzers A, der die Nachricht signiert

- Verifikation der Signatur der Nachricht m:

V (m, s, ÖSA) = true ?

V: Verifikationsfunktion
ÖSA: öffentlicher Schlüssel des Nutzers A, der die Nachricht signiert ha

Digitale Signaturen und Zertifikate
→ Digitale Signatur (2/3)

- Public-Key-Verfahren haben eine relativ **hohe Verarbeitungszeit** für eine Operation.
  - Zu signierende Nachricht m, muss kleiner als die verwendete Schlüsselgröße sein.
  - 100 MB = 800.000.000 Bit
    ➔ ca. 400.000 Operationen bei 2.048 Bit Schlüssellänge
    ➔ ca. 11 h bei 100 ms pro Operation
- Die **Zusammengehörigkeit** von Einzelsignaturen ist nicht gegeben.

Digitale Signaturen und Zertifikate
→ Digitale Signatur (3/3)

- Lösung: **One-Way-Hashfunktion**

$$\mathbf{AV (h_m = H (m), s, ÖSA) = true}$$

h_m: Hashwert der Nachricht m
H: One-Way-Hashfunktion
AV: Angepasste Verifikationsfunktion

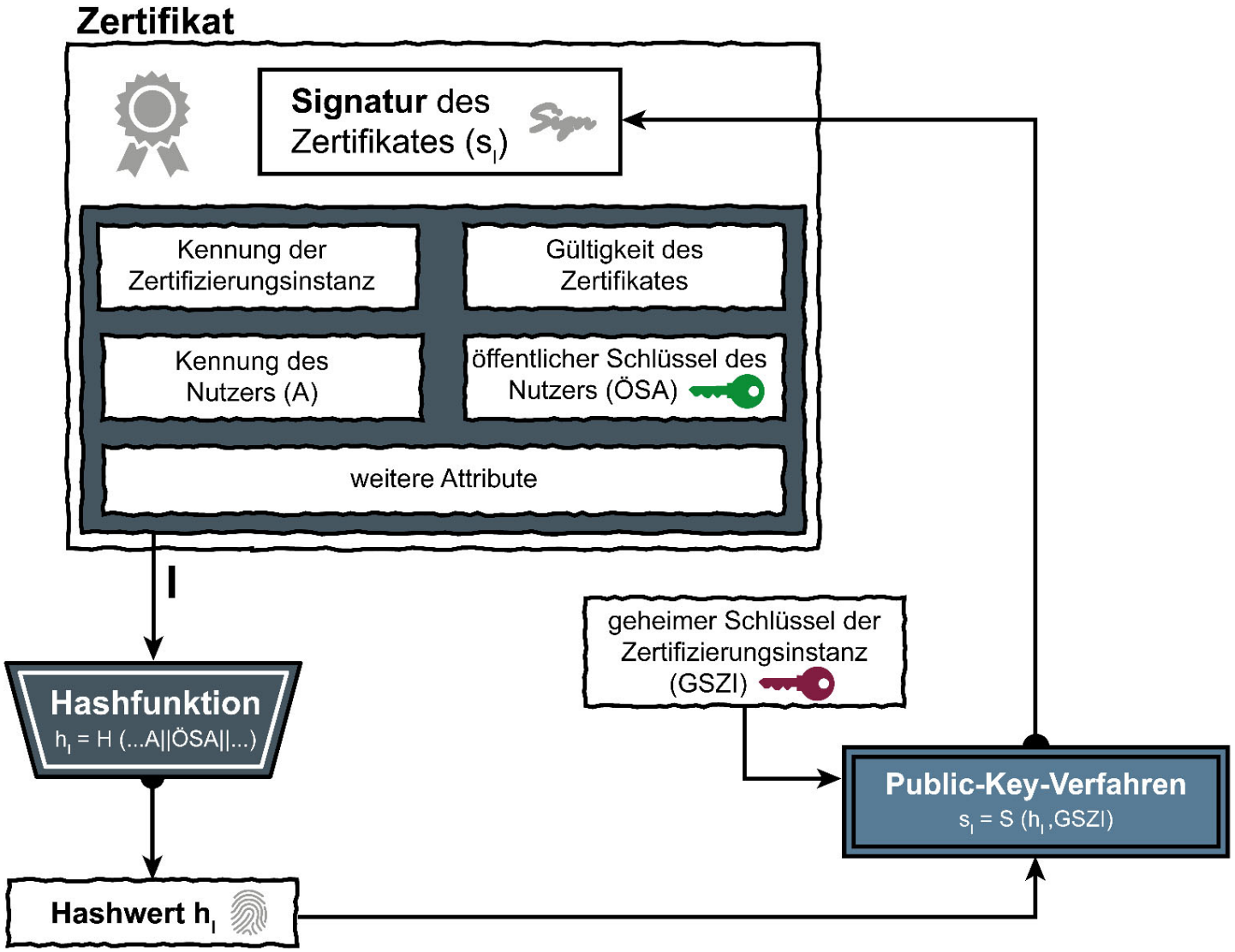
- **Vorteile:**
  - Signierung von **beliebig langen** Nachrichten möglich.
  - Geringere **Zeit** für die Erstellung der Signatur nötig.
  - Gewährleistung der **Integrität** - Jedes Bit der Nachricht ist in die digitale Signatur eingeschlossen!

Digitale Signaturen und Zertifikate
→ Digitale Zertifikate

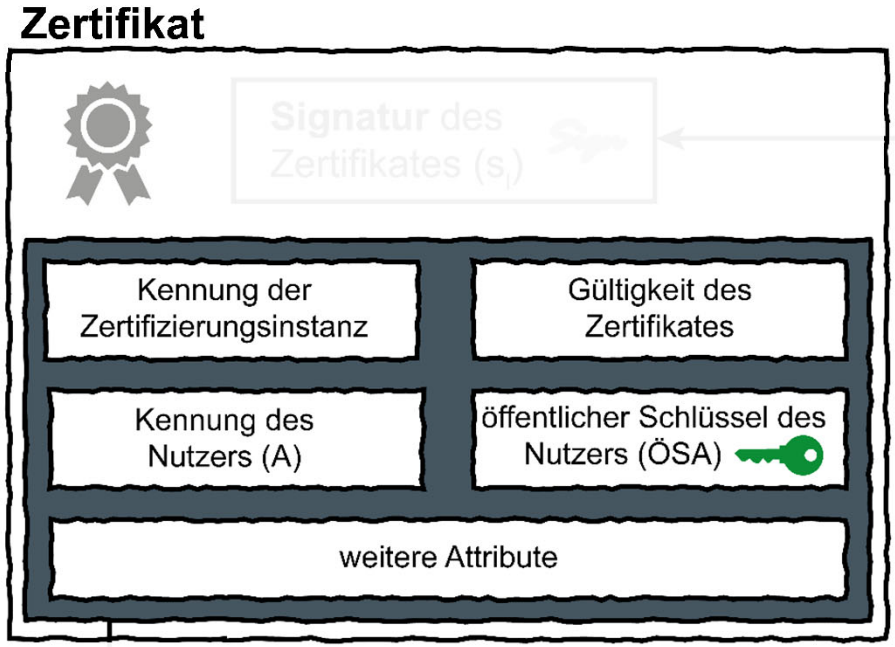
- Mit Hilfe von elektronischen Zertifikaten können:
  - **Attribute** von Nutzern überprüfbar nachgewiesen werden,
  - die **Authentizität** von öffentlichen Schlüsseln nachgewiesen werden.

- Ausgestellt werden elektronische Zertifikate durch eine **Zertifizierungsinstanz**:
  - Spezialisierte allgemeine Anbieter für Vertrauensdienste, Berufsverbände (z.B. Notare, Steuerberater/ Wirtschaftsprüfer, Ärzte/Krankenschwerstern/Hebammen), Personal und IT-Abteilungen von Unternehmen, Behörden.
  - Wirksame Prüfung aller relevanten Daten (z.B. Identität, Ausweis, Urkunden und weitere Attribute).

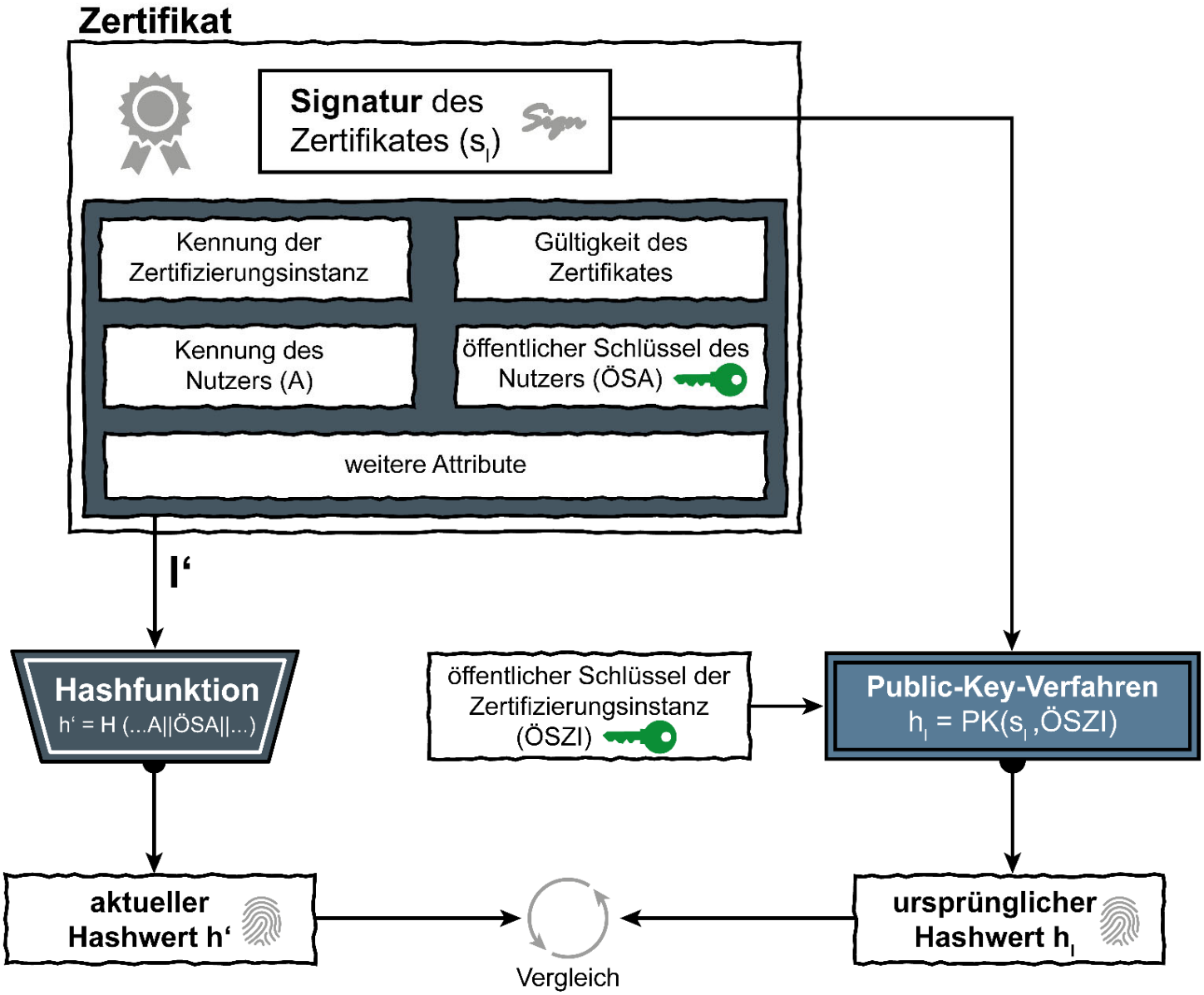
Digitale Signaturen und Zertifikate
→ Erstellung eines digitalen Zertifikates



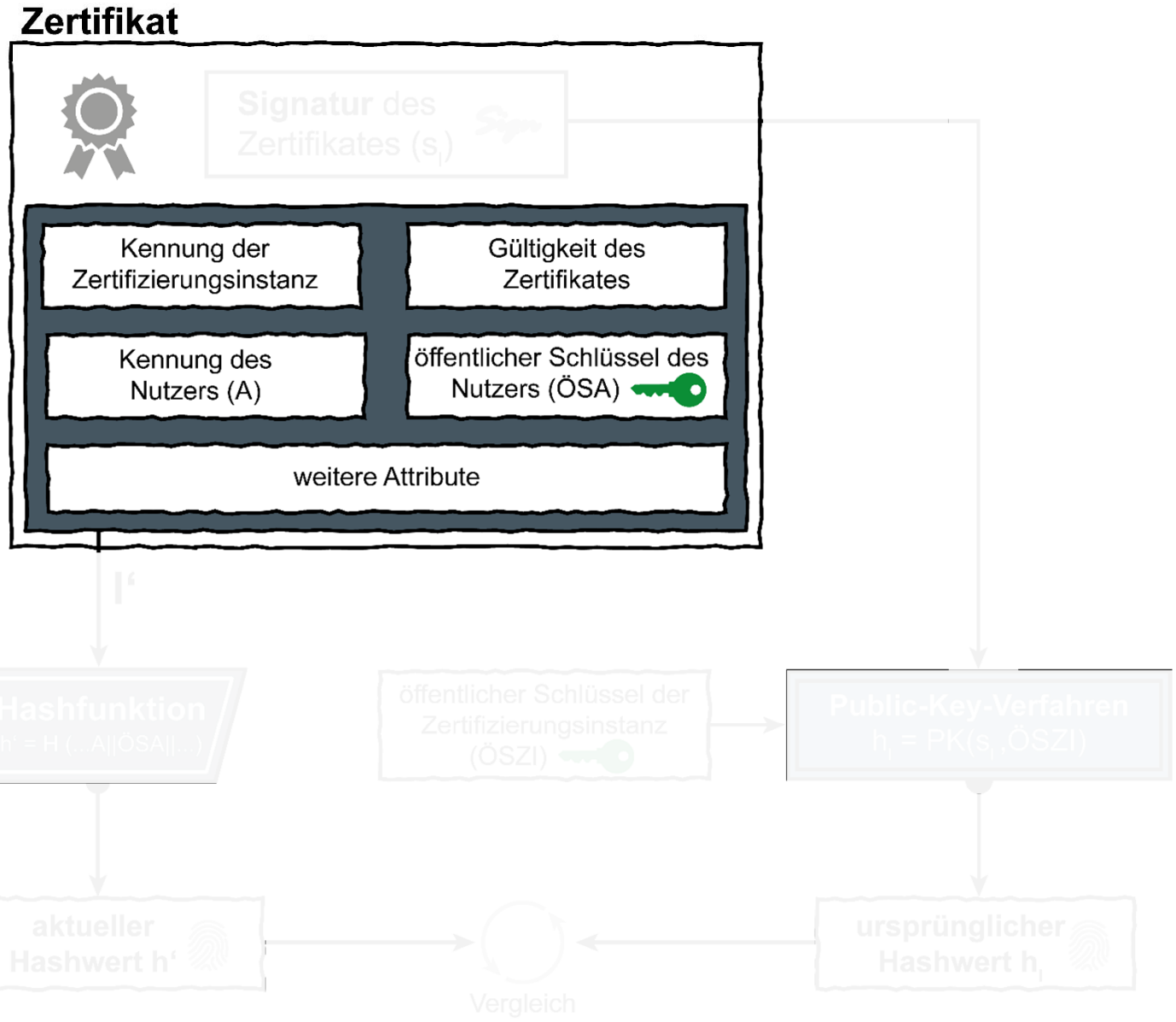
Digitale Signaturen und Zertifikate
→ Erstellung eines digitalen Zertifikates



Digitale Signaturen und Zertifikate
→ Verifikation eines digitalen Zertifikates



Digitale Signaturen und Zertifikate
→ Verifikation eines digitalen Zertifikates



Signatur, Zertifikate und PKI
→ Inhalt

- Ziele und Ergebnisse der Vorlesung
- Digitale Signaturen und Zertifikate
- **Public-Key-Infrastrukturen**
- Gesetzlicher Hintergrund
- PKI-enabled Application
- Zusammenfassung

Public-Key-Infrastrukturen
→ Idee und Definition (1/2)

- **Verwalten** von Zertifikaten mit öffentlichen Schlüsseln und weiteren Attributen über deren gesamten **Lebenszyklus**:
  - Erstellung, Aufbewahrung, Verwendung, Löschung.
  - Wichtig: Verifizierung der ursprünglichen Identität der Inhaber.

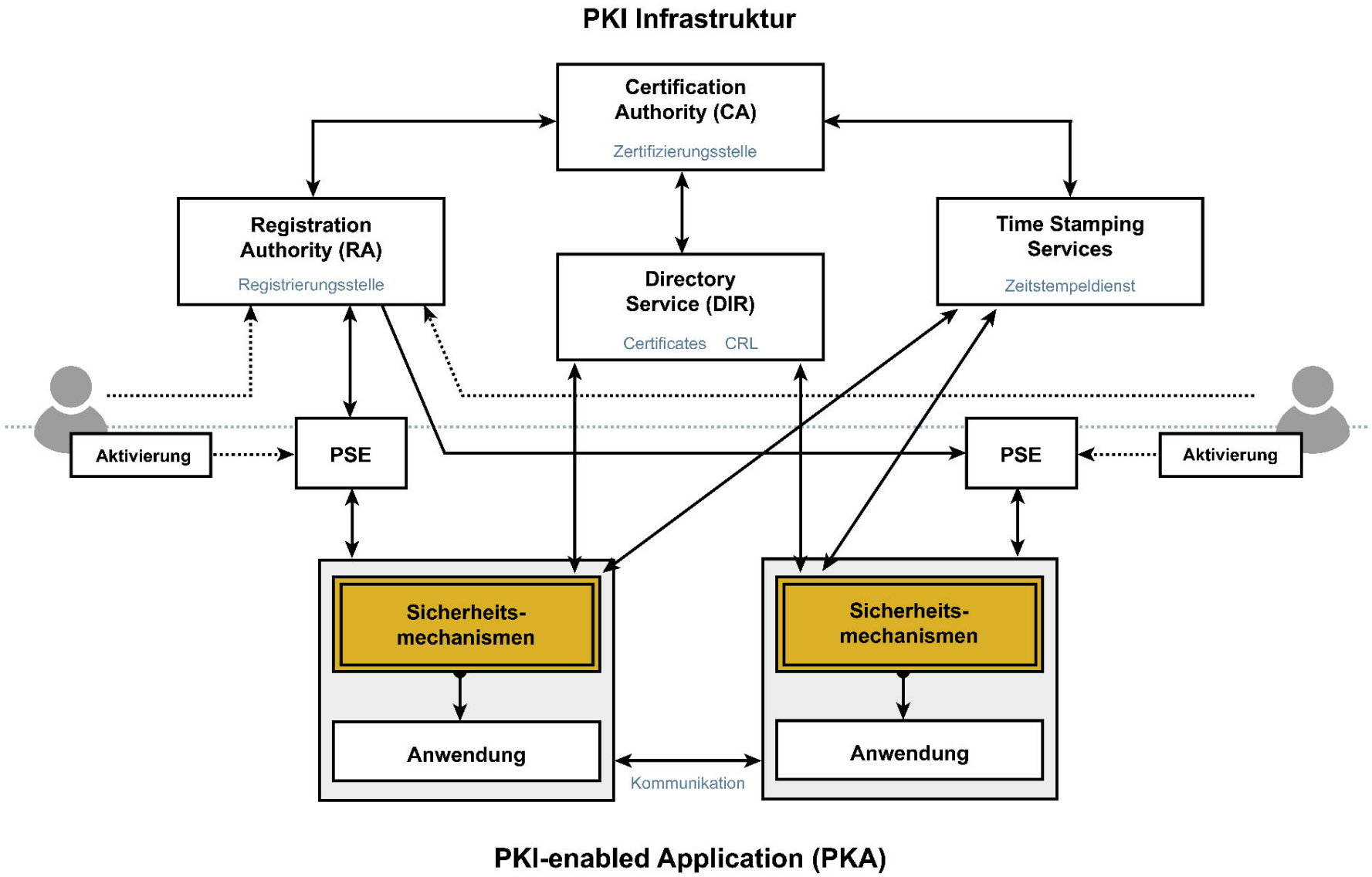
- **Analogie:** Standesamt und Einwohnermeldeamt.

- **Bestandteile einer PKI:**
  - Hardware
  - Software
  - Regelwerk

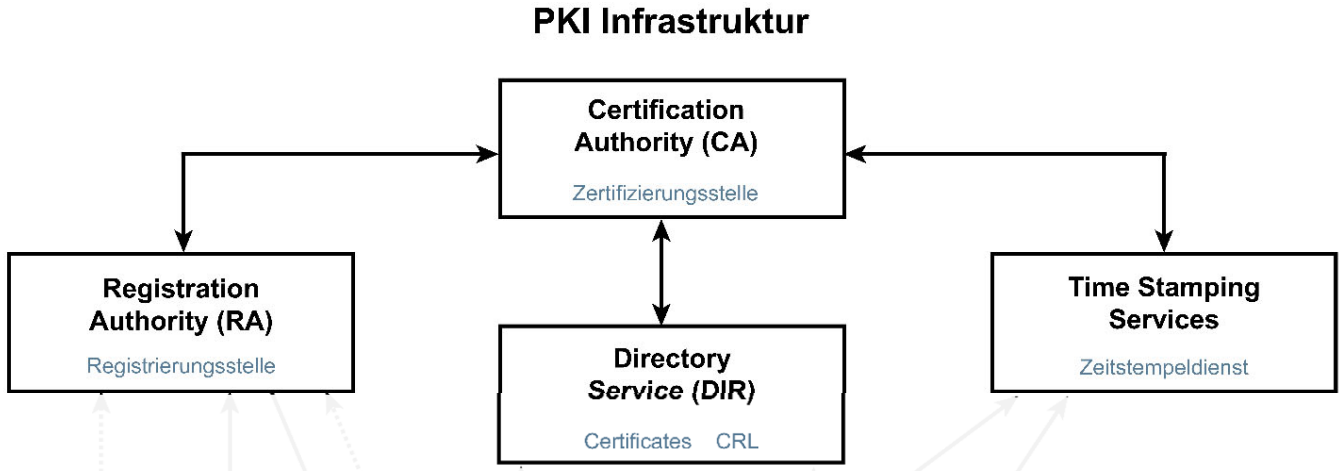
Public-Key-Infrastrukturen
→ Idee und Definition (2/2)

Cyber-Sicherheitsbedürfnisse		Cyber-Sicherheitsmechanismen
Authentizität	→	Signatur
Integrität	→	Signatur
Verbindlichkeit	→	Signatur
Einmaligkeit	→	TimeStamp
Vertraulichkeit	→	Verschlüsselung

Public-Key-Infrastrukturen
→ Aufbau und Funktionsweise (1/4)



Public-Key-Infrastrukturen
→ Aufbau und Funktionsweise (1/4)



Public-Key-Infrastrukturen
→ Aufbau und Funktionsweise (2/4)

- **Registration Authority (RA):**
  - Schnittstelle zwischen dem PKI-Nutzer und der Certification Authority (CA).
  - Private oder öffentliche Einrichtung (z.B. Berufsverbände, Unternehmen, Behörden und öffentliche Dienstanbieter).
  - Anträge auf Zertifizierung erfassen.
  - Identität der Antragsteller gemäß des Regelwerks prüfen.

- **Certification Authority (CA):**
  - Vergabe von eindeutigen digitalen Identitäten.
  - Erzeugung von Zertifikaten.
  - Verwaltung von Schlüsselpaaren pro Nutzer.

Public-Key-Infrastrukturen
→ Aufbau und Funktionsweise (3/4)

- **Directory Service (DIR):**
  - Verzeichnisdienst zur Verwaltung der Zertifikate.
  - Öffentlich zugreifbar.

- **Certificate Revocation List (CRL):**
  - Sperrliste für zurückgezogene oder kompromittierte Schlüssel/Zertifikate.
  - Vor jeder Verifikation sollte ein Abgleich mit der Sperrliste erfolgen.

- **Time Stamping Service:**
  - Erstellung von gesicherten Zeitsignaturen gemäß des Regelwerks.

Public-Key-Infrastrukturen
→ Aufbau und Funktionsweise (4/4)

- **Personal Security Environment (PSE):**
  - Sammlung aller sicherheitsrelevanten Daten eines Teilnehmers.
    - Geheimer Schlüssel des Nutzers,
    - öffentlicher Schlüssel der Zertifizierungsinstanz,
    - ggf. Zertifikate seiner Kommunikationspartner.
  - Mögliche Formen: Software, Smartcards, USB-Token, allgemeine Sicherheits-Module, SIM-Karte im Smartphones, TPM, usw.

- **PKI-enabled Application (PKA):**
  - Anwendungen, die auf Basis der Sicherheitsmechanismen einer PKI umgesetzt werden (z.B. Dokumentenverschlüsselung, Zahlungssysteme, IPSec-Kommunikation, …).

Public-Key-Infrastrukturen
→ Wirksamkeit (1/2)

- Sichere und vertrauenswürdig umgesetzte PKIs haben eine hohe Wirksamkeit bezüglich der Cybersicherheit.
- Unsicher gespeicherte Schlüssel sind ein Sicherheitsrisiko.
- Aus diesem Grund werden in der Regel Smartcards oder USB-Sicherheitstoken verwendet.
- Restrisiko durch Malware kann mit externen Lesegeräten und Tastaturen minimiert werden.

Public-Key-Infrastrukturen
→ Wirksamkeit (2/2)

- Es können drei Kategorien an Lesegeräten unterschieden werden, die einen unterschiedlichen Level an Sicherheit und damit an Wirkung gegen Angriffe zur Verfügung stellen:

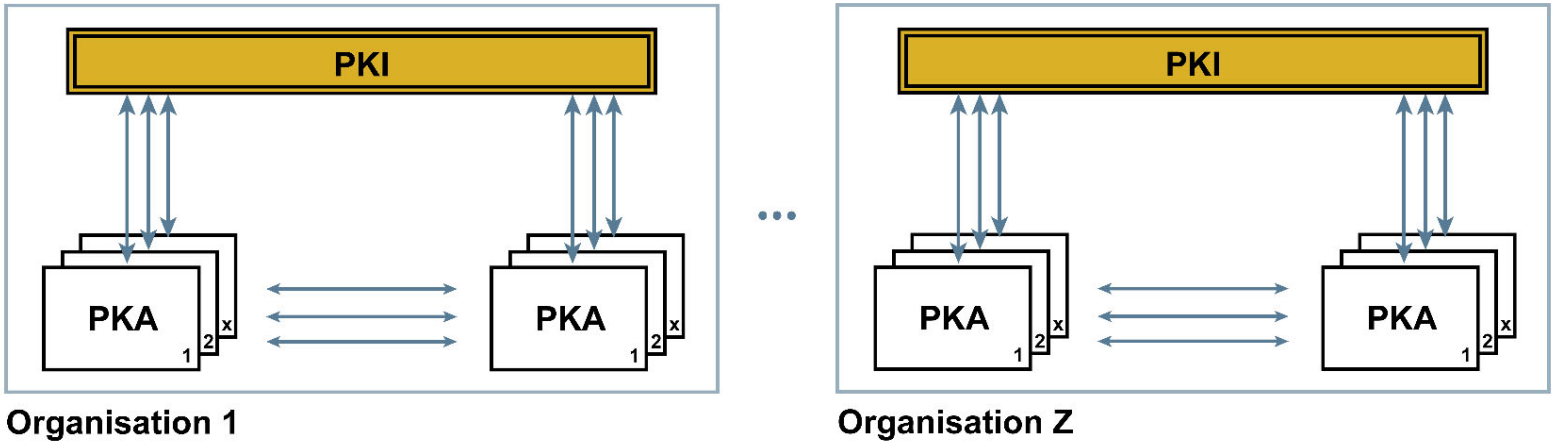
- **1. Basisleser:**
  - Anzeige und Eingabe über das selbe IT-System des Nutzers.
  - Hohes Restrisiko durch Malware.

- **2. Standardleser**
  - Anzeige und Eingabe über externes IT-System.

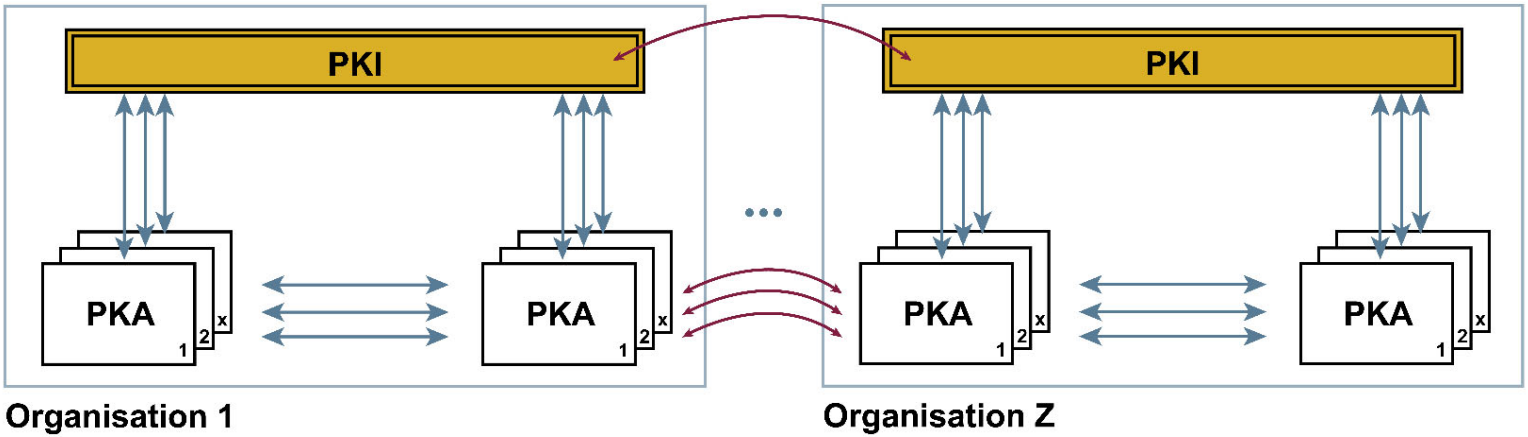
- **3. Komfortleser**
  - Zertifizierter Standardleser.
  - Höheres Vertrauenslevel.

Public-Key-Infrastrukturen
→ PKI Konzepte (1/2)

- Geschlossene und dezentrale PKI-Systeme:

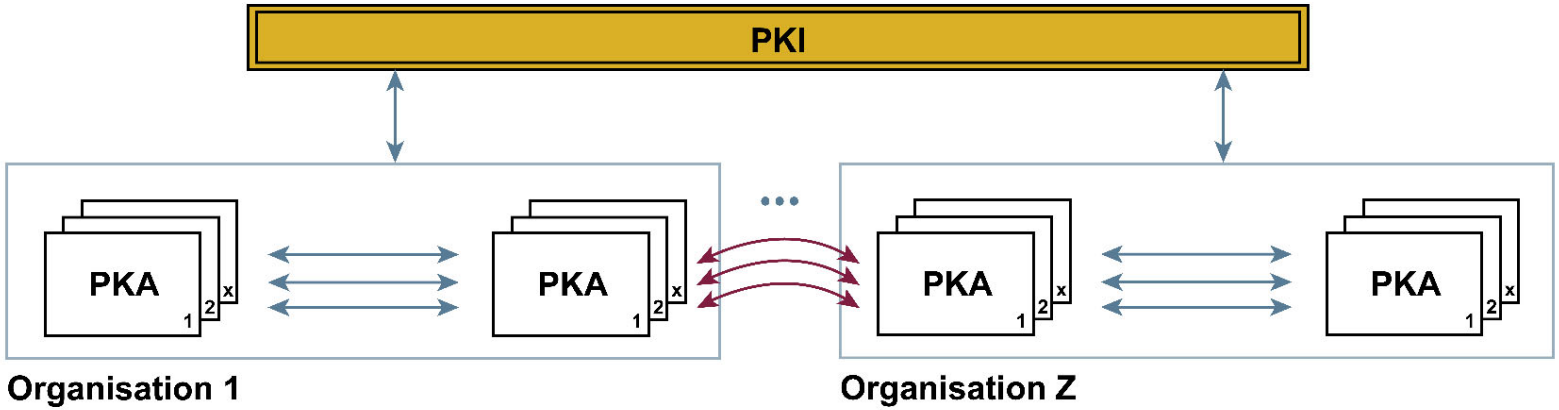


- Offene und dezentrale PKI-Systeme:



Public-Key-Infrastrukturen
→ PKI Konzepte (2/2)

- Offene, zentrale PKI-Systeme:



Public-Key-Infrastrukturen
→ Probleme in der Praxis (1/3)

- **Probleme bei geschlossenen PKI-Systemen:**
  - PKI-Dienstleistungen können nur innerhalb einer Organisation verwendet und nicht für die Kommunikation nach außen genutzt werden.
  - In der Praxis existieren jedoch viele organisationsübergreifende Prozesse.

- **Probleme bei offenen PKI-Systemen:**
  - Abgleich der verschiedenen organisationsspezifischen Regelwerke nötig.
  - Ziel ist die Schaffung einer gemeinsamen, verbindlichen Vertrauensbasis (Level of Trust).
  - Viele unterschiedliche, teilweise sehr komplexe Standards.

Public-Key-Infrastrukturen
→ Probleme in der Praxis (2/3)

- **Unterschiedliche Verantwortung für PKIs und PKAs in Unternehmen:**
  - Verständigung über verschiedene Abteilungen hinweg nötig.
  - Aufwand in großen Unternehmen höher.

- **Henne-Ei-Problem:**
  - PKIs benötigen konsequenten Einsatz der bestehenden Technologien und die Umsetzung der Security Regelwerke.
  - Realität: Organisationen können sich nur schwer auf den Abgleich ihrer individuellen Cyber-Sicherheitskonzepte einigen.
  - Dadurch gestaltet sich der Aufbau eines gemeinsamen „Level of Trust“ langwierig, und längst fällige Entscheidungen werden nicht getroffen.

Public-Key-Infrastrukturen
→ Probleme in der Praxis (3/3)

- **Hoher personeller und organisatorischer Aufwand:**
  - Sensibilisierung der Nutzer für die Cyber-Sicherheit.
  - Schulung der Nutzer für die Produkte und die Planung.
  - Durchführung des Roll-Out.

- **Key-Recovery bei der Verschlüsselung:**
  - Verfahren zur Entschlüsselung benötigt, falls:
    - Technischen Defekte auftreten,
    - PSE verloren gehen,
    - Mitarbeiter aus dem Unternehmen ausscheiden.

Public-Key-Infrastrukturen
→ Umsetzungskonzepte (1/4)

- Die folgenden vier Kernsätze können als Grundlage für die erfolgreiche Realisierung eines PKI-Systems gelten:
  - Verschiedene Anwendungen haben unterschiedliche Cyber-Sicherheitsbedürfnisse.
  - Unterschiedliche Cyber-Sicherheitsbedürfnisse lassen sich isoliert einfacher verwirklichen.
  - Isolierte Lösungen haben einen klaren Fokus.
  - Ein klarer Fokus verringert die auftretenden Probleme und ermöglicht eine schnellere, einfachere und kostengünstigere Umsetzung.

Public-Key-Infrastrukturen
→ Umsetzungskonzepte (2/4)

- **Umsetzungskonzept „TLS/SSL“:**
  - Vertrauliche Kommunikation zwischen Client und Server.
  - TLS/SSL Infrastruktur ist gegeben:
    - Web Server,
    - Clients,
    - mehrere hundert PKIs,
    - Open Source Bibliotheken,
    - TLS/SSL-Accelerator-Lösungen.
  - 2018 wurden schon mehr als 80 % der IP-Pakete mit TLS/SSL im Internet verschlüsselt.

Public-Key-Infrastrukturen
→ Umsetzungskonzepte (3/4)

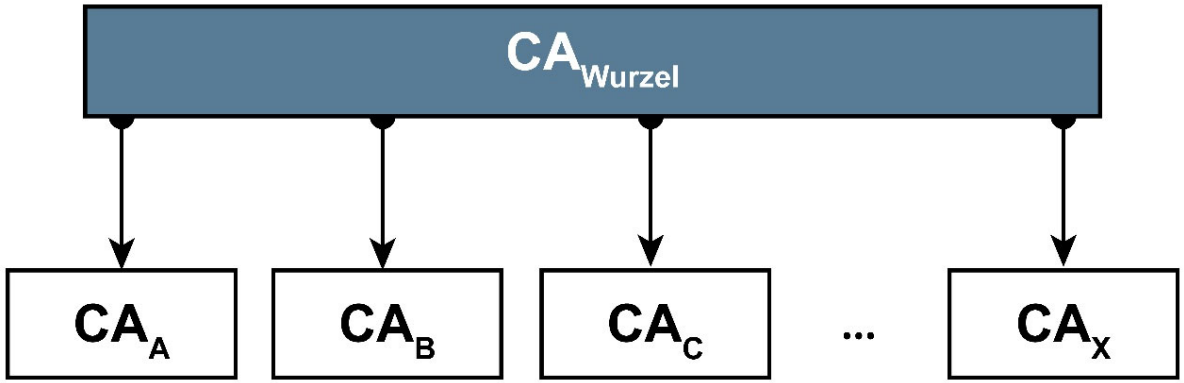
- **Umsetzungskonzept „E-Mail-Sicherheit“:**
  - Zu schützende Unternehmensdaten sollen personenorientiert und vertraulich ausgetauscht werden.
  - Das gegenseitige Wissen um die Identität der Kommunikationspartner ist von zentraler Bedeutung.
  - Insbesondere wenn via E-Mail Prozesse mit nachfolgenden Kosten (Bestellungen, Wareneinkauf, ...) ausgelöst werden, liegt die Verbindlichkeit im Interesse der Unternehmen.
  - Mailprogramme sind den Nutzern bekannt und vertraut.
  - Sicherheitsrelevante Funktionen müssen so eingepasst werden, dass der Nutzer sich nur einem Mindestmaß an neuen Funktionalitäten gegenübersieht und jederzeit Klarheit über die nötigen Arbeitsschritte und ihre Folgen hat.

Public-Key-Infrastrukturen
→ Umsetzungskonzepte (4/4)

- **Umsetzungskonzept „Verbindlicher Austausch von Transaktionsdaten“:**
  - Transaktionsdaten sind 'besondere' Kommunikationsdaten, da sich aus ihnen in der Regel kostenrelevante Aktionen ableiten.
  - Für den Empfänger wie für den Sender steht die Verbindlichkeit im Mittelpunkt.
  - Diese Anwendungen sind meist firmen- bzw. gerätebezogen und basieren auf geschlossenen Systemen (z.B. der Austausch von Rechnungsdaten zwischen Telekommunikationsanbietern und ihren Partnerunternehmen).
  - Die Bandbreite reicht von kleinen Datenmengen pro Monat bis hin zu einer hohen Anzahl von Transaktionen pro Minute.
  - Der Fokus liegt auf der möglichst nahtlosen Integration in bestehende Workflows.

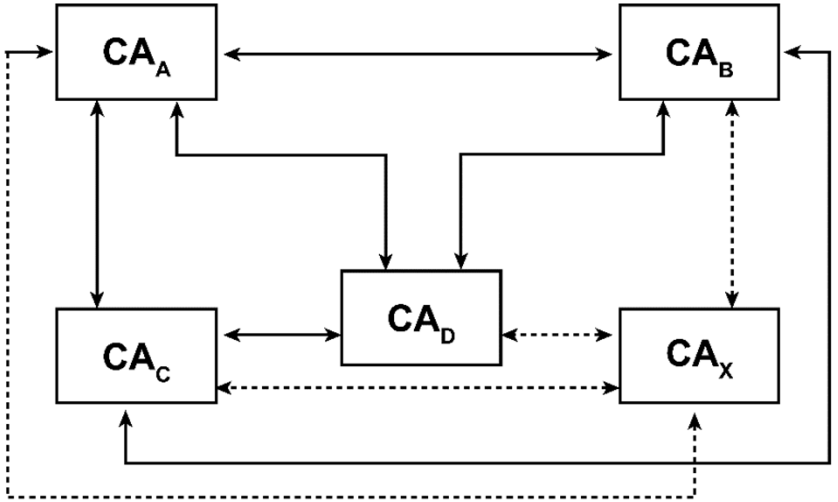
Public-Key-Infrastrukturen
→ Vertrauensmodelle (1/3)

- **Übergeordnete CA (Wurzel-CA, Root CA):**
  - Wurzel-CA generiert Zertifikate der öffentlichen Schlüssel der untergeordneten CAs.
  - Der öffentliche Schlüssel der Wurzel-CA ist im PSE untergebracht oder wird als Zertifikat zum Abrufen angeboten.
  - In den meisten Fällen akzeptieren Unternehmen, Organisationen oder Länder keine derartige Unterordnung.
  - Nur in großen, geschlossenen PKI-Systemen etabliert.



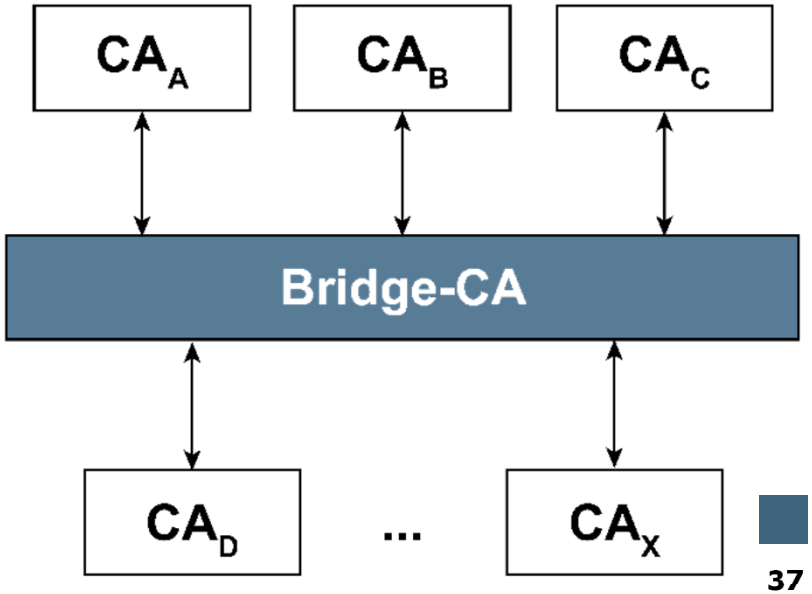
Public-Key-Infrastrukturen
→ Vertrauensmodelle (2/3)

- **n:n-Cross-Zertifizierung:**
  - Jede CA tauscht ihre öffentlichen Schlüssel selbstständig mit jeder anderen CA aus.
  - Authentischer Austausch der öffentlichen Schlüssel aufwendig.
  - Multiple Vertragsverhandlungen nötig.
  - Abweichende Verträge und Vereinbarungen zwischen den beteiligten Betreibern möglich.
  - Nur bei kleinen Gruppenunabhängiger PKI-Betreiber etabliert, und auch dort nur in abgegrenzten Geschäftsprozessen.



Public-Key-Infrastrukturen
→ Vertrauensmodelle (3/3)

- **1:n Cross-Zertifizierung (Bridge CA):**
  - Geringer Verwaltungsaufwand, da es für jede CA nur einen Vertragspartner gibt.
  - Entscheidungsfreiheit über die passende Vertrauenskette.
  - Bridge CA fungiert als zentrale Vermittlungsinstanz zwischen den beteiligten Organisationen → Geeignete Policy benötigt.
  - CAs übergeben authentisch ihre öffentlichen Schlüssel an die Bridge CA.
  - Bridge CA signiert eine Tabelle der öffentlichen Schlüssel aller beteiligten CAs.
  - Die eigene CA stellt dann all ihren Nutzern den öffentlichen Schlüssel der Bridge CA als Zertifikat zur Verfügung.



Signatur, Zertifikate und PKI
→ Inhalt

- Ziele und Ergebnisse der Vorlesung
- Digitale Signaturen und Zertifikate
- Public-Key-Infrastrukturen
- **Gesetzlicher Hintergrund**
- PKI-enabled Application
- Zusammenfassung

Gesetzlicher Hintergrund → eIDAS (1/7)

- EU-Verordnung 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS).
  - Gleichstellung, Interoperabilität, gegenseitige Anerkennung der **Vertrauensdienste** der Mitgliedsstaaten.
- Für alle in der EU niedergelassenen Vertrauensdienstanbieter (VDA).
  - Ausgenommen: Vertrauensdienste innerhalb geschlossener Nutzergruppen, wie z.B. interne Unternehmenslösungen.
- In Deutschland umgesetzt durch:
  - Signaturgesetz (SigG)
  - Signaturverordnung (SigV)

Gesetzlicher Hintergrund
→ eIDAS (2/7)

- Das Vertrauen durch eIDAS ist untrennbar mit der Rechtssicherheit verbunden.
  - Ein elektronisches Dokument soll in der EU den gleichen Stellenwert erhalten wie ein analoges.
- Unterteilung in qualifizierte und nicht-qualifizierte VDA.
  - Freiwillige Akkreditierung alle drei Jahre möglich (Konformitätsbewertung).
- Art. 13: Zusätzliches Vertrauen durch freiwilliges EU-Vertrauenssiegel (Analogie: „IT Security made in Germany“ Qualitätssiegel der TeleTrusT).

Gesetzlicher Hintergrund
→ eIDAS (3/7)

- Art. 28: Suspendierung von qualifizierten Zertifikaten möglich.

- Art. 35-40: Elektronische Siegel als Pendant zu elektronische Signaturen.
  - Signaturen → natürliche Personen
  - Siegel → Organisationen

- **Elektronische Fernsignaturen:**
  - Sichere Signaturerstellungseinheit (SSEE) befindet sich beim qualifizierten VDA.
  - Auslöser der Signatur wird mit technischen Mitteln verlängert.
  - VDA muss geeignete Cybersicherheitsmechanismen umsetzen.

Gesetzlicher Hintergrund
→ eIDAS (4/7)

- Art. 11, 13: Haftung und Beweislast:
  - Qualifizierte VDA sind in der Nachweispflicht.
  - Bei nicht-qualifizierten VDA liegt die Nachweispflicht hingegen beim Kunden.
  - Der VDA haftet, wenn er die in der eIDAS-Verordnung genannten Pflichten nicht eingehalten hat (z.B. wenn die Dienste nicht dem neusten Stand der Technik entsprechen).
  - VDA kann Haftung im Vorfeld beschränken.

Gesetzlicher Hintergrund
→ eIDAS (5/7)

- Art. 43-44: Elektronisches Einschreiben - Anforderungen:
  - Identifizierung des Absenders mit hohem Maß an Vertrauenswürdigkeit.
  - Identifizierung des Empfängers vor Zustellung der Daten.
  - Absenden und Empfang ist durch fortgeschrittene elektronische Signatur oder ein fortgeschrit-tenes elektronisches Siegel eines qualifizierten VDA vor Veränderung geschützt.
  - Jede Veränderung von Daten wird deutlich angezeigt.
  - Zeit und Datum von Versand, Empfang oder Änderung der Daten wird durch qualifizierte elekt-ronische Zeitstempel angezeigt.

Gesetzlicher Hintergrund
→ eIDAS (6/7)

- De-Mail:
  - Es versieht immer der akkreditierte Anbieter selbst die Nachrichten mit einer qualifizierten Signatur (Fernsignatur).
  - Überall, wo in eIDAS qualifizierte Zeitstempel vorgesehen sind, benutzt De-Mail Prüfsummen und qualifizierte Signaturen.
  - De-Mail schreibt zwingend eine Transportverschlüsselung zwischen den Anbietern vor.
  - De-Mail überlässt es den Anbietern, eine sichere Dokumentenablage anzubieten.
  - De-Mail ist aktuell also nicht vollständig eIDAS-konform.

Gesetzlicher Hintergrund
→ eIDAS (7/7)

- Art. 19: Sicherheitsanforderungen an Vertrauensdienstanbieter:
  - Alle qualifizierten und nicht-qualifizierten VDA müssen Cybersicherheitsmechanismen gemäß dem Stand der Technik implementieren.
  - Sicherheitsvorfall müssen innerhalb von 24 Stunden an die zuständige nationale Stelle bzw. Datenschutzbehörde sowie die betroffenen natürlichen oder juristischen Personen gemeldet werden.
  - Betreffen Cybersicherheitsvorfälle mehrere Mitgliedsstaaten, so müssen die Aufsichtsstellen der betroffenen Mitgliedsstaaten und die ENISA davon in Kenntnis gesetzt werden.
  - Aufsichtsstelle entscheidet über Veröffentlichung des Vorfalls.

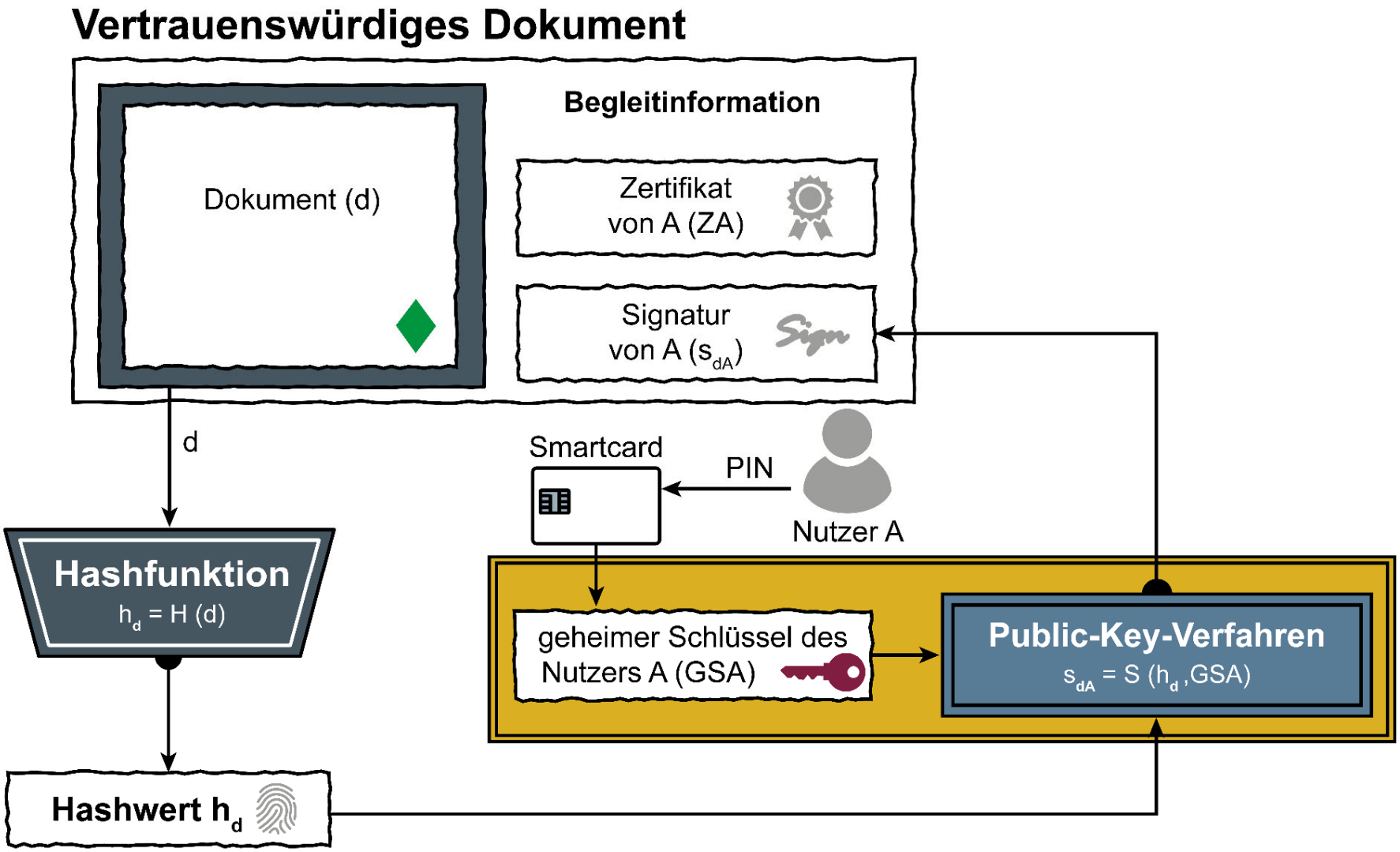
Signatur, Zertifikate und PKI
→ Inhalt

- Ziele und Ergebnisse der Vorlesung
- Digitale Signaturen und Zertifikate
- Public-Key-Infrastrukturen
- Gesetzlicher Hintergrund
- **PKI-enabled Application**
- Zusammenfassung

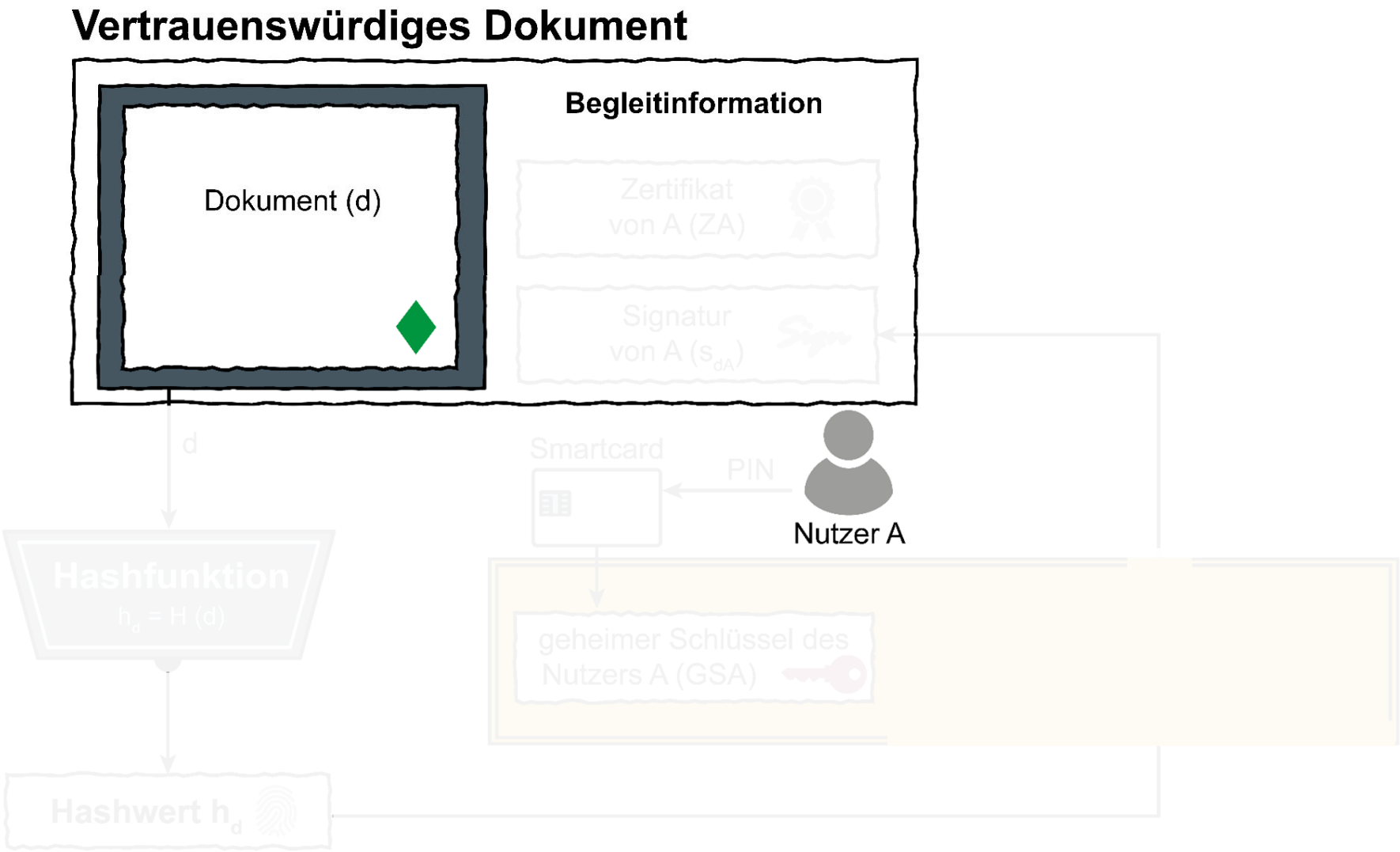
PKI-enabled Application
→ E-Mail Sicherheit (1/8)

- Eine Information wurde früher entweder auf einer Schreibmaschine getippt oder mithilfe eines Textverarbeitungssystems in ein IT-System eingegeben und anschließend ausgedruckt.
- Der Ausdruck wurde unterschrieben, in einen Briefumschlag gesteckt und vertraulich an den gewünschten Empfänger gesendet.
- Der Empfänger erkannte an der Unversehrtheit des Umschlags, dass die Information vertraulich übermittelt worden war.
- Nach dem Öffnen des Briefes konnte der Empfänger an der eigenhändigen Unterschrift die Echtheit des Absenders oder des Autors überprüfen.
- Die eigenhändige Unterschrift ist zudem eine rechtsgültige Unterschrift.
- E-Mail-Sicherheit bedeutet, die gleiche Sicherheit bei Mails zu haben, die auch für Briefe gilt.

PKI-enabled Application
→ E-Mail Sicherheit (2/8)



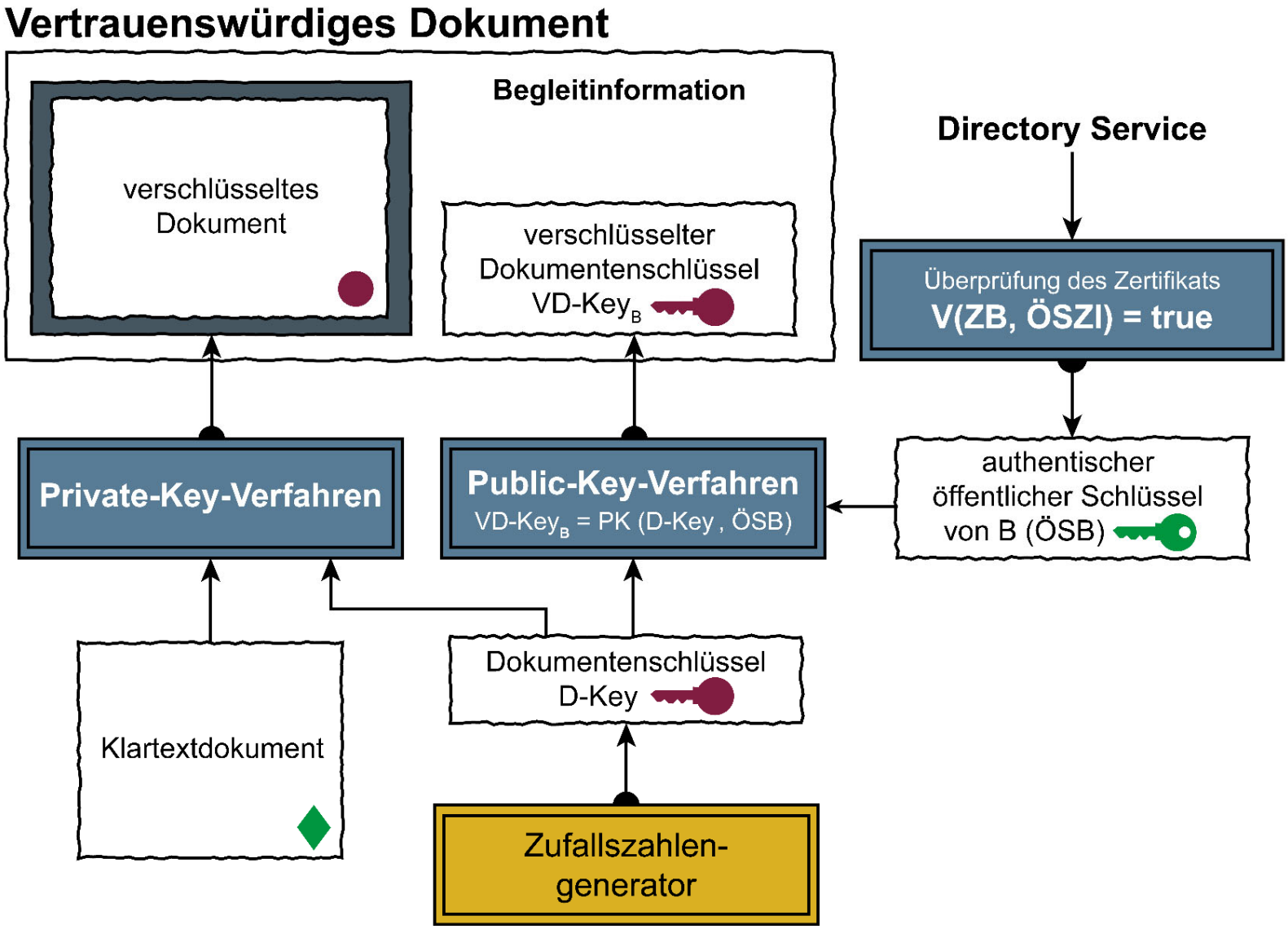
PKI-enabled Application
→ E-Mail Sicherheit (2/8)



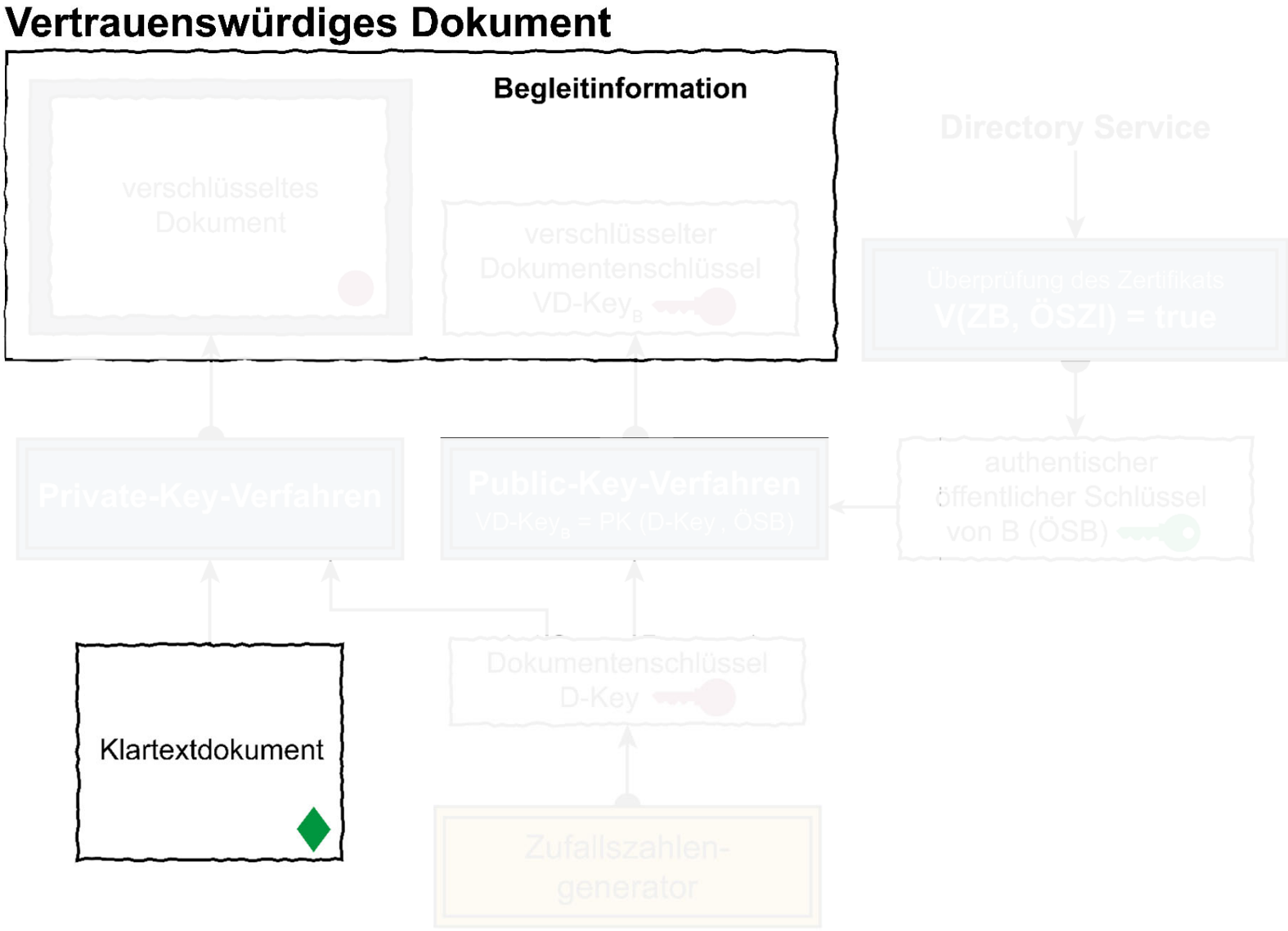
PKI-enabled Application
→ E-Mail Sicherheit (3/8)

- Digitaler Zeitstempel:
  - Die Beweiskraft eines elektronischen Dokuments hängt häufig zusätzlich auch vom Zeitpunkt seiner Erstellung ab.
  - Da die Uhren und Zeitfunktionen sich in handelsüblichen IT-Systemen und Betriebssystemen ohne Probleme verstellen lassen, kann die Urzeit nicht für eine vertrauenswürdige Zeitangabe bei der digitalen Signatur angeben werden.
  - Ein Zeitstempel benötigt eine digitale Bescheinigung einer Zertifizierungsstelle.
  - Sie bestätigt, dass das Dokument zum angegebenen Zeitpunkt ihr vorgelegen hat, indem sie den Zeitstempel digital signiert.

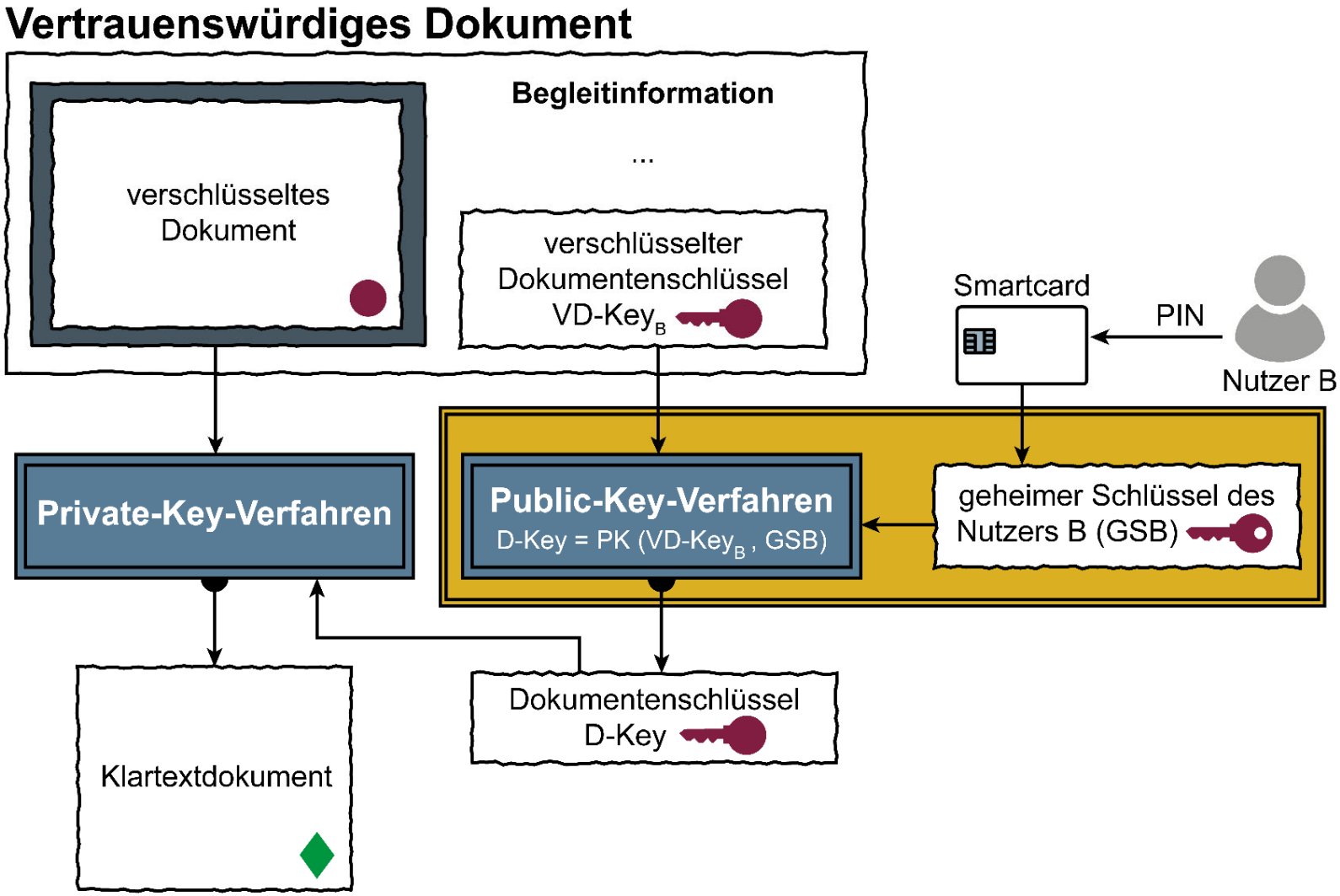
PKI-enabled Application
→ E-Mail Sicherheit (4/8)



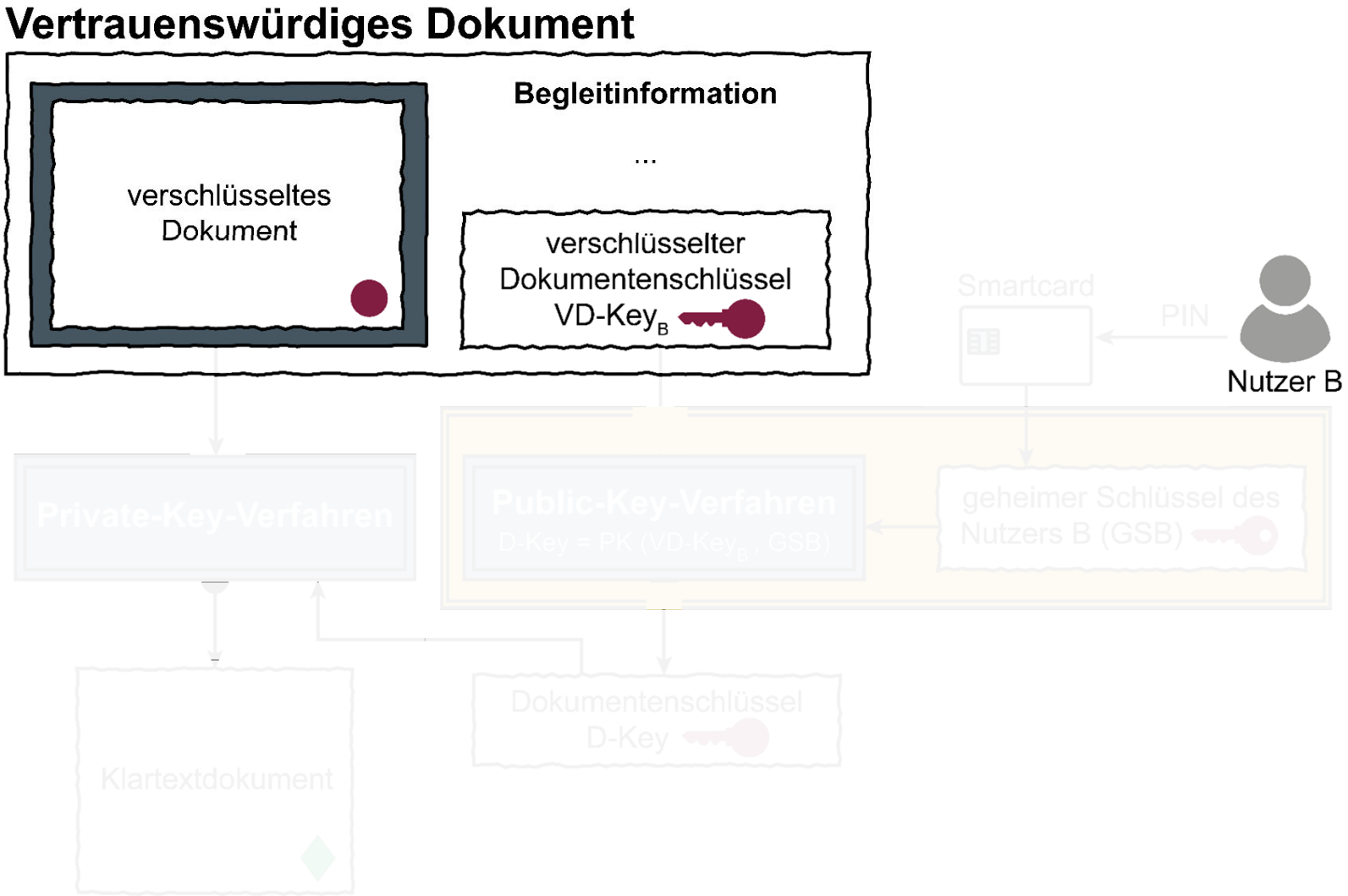
PKI-enabled Application
→ E-Mail Sicherheit (4/8)



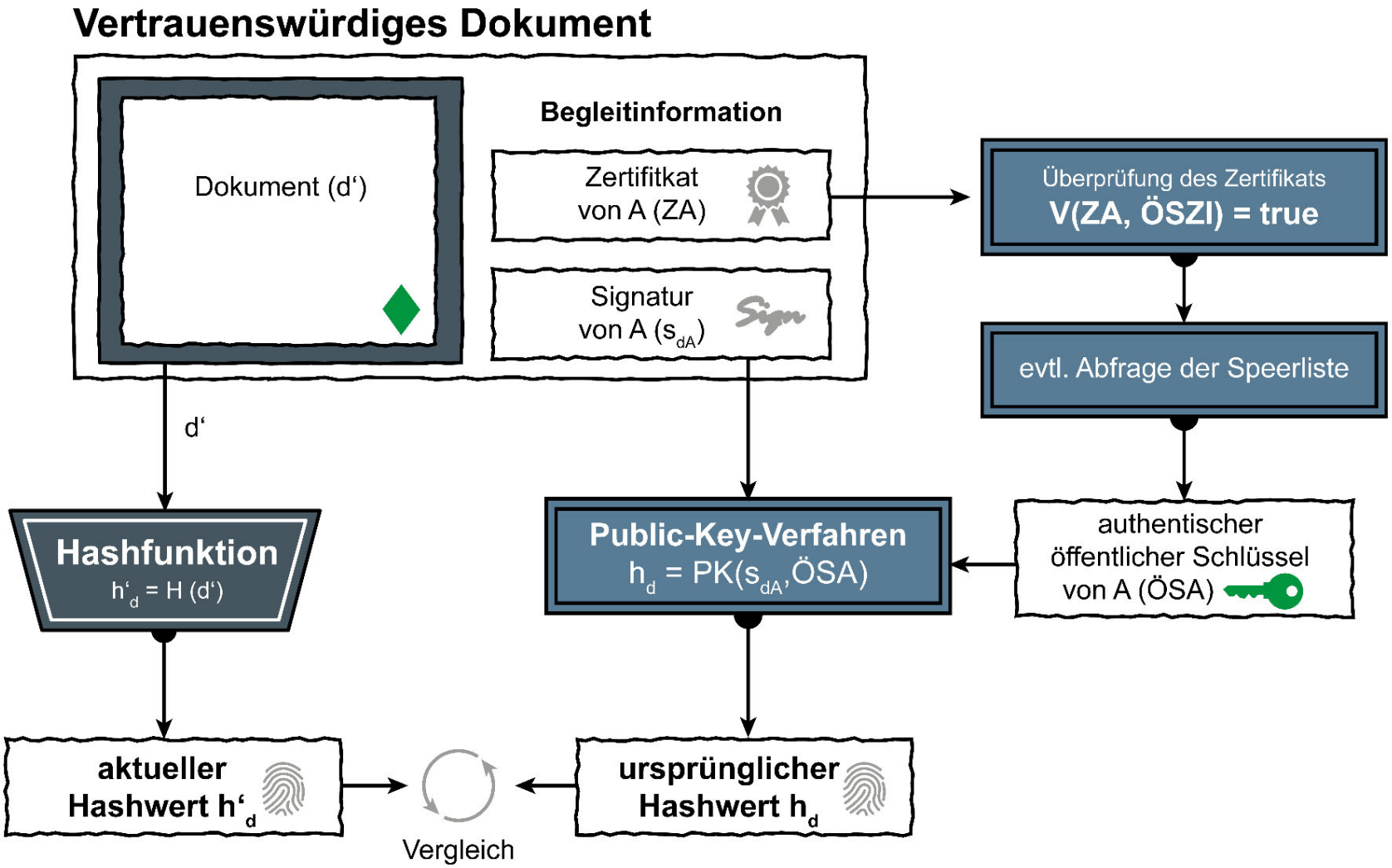
PKI-enabled Application
→ E-Mail Sicherheit (5/8)



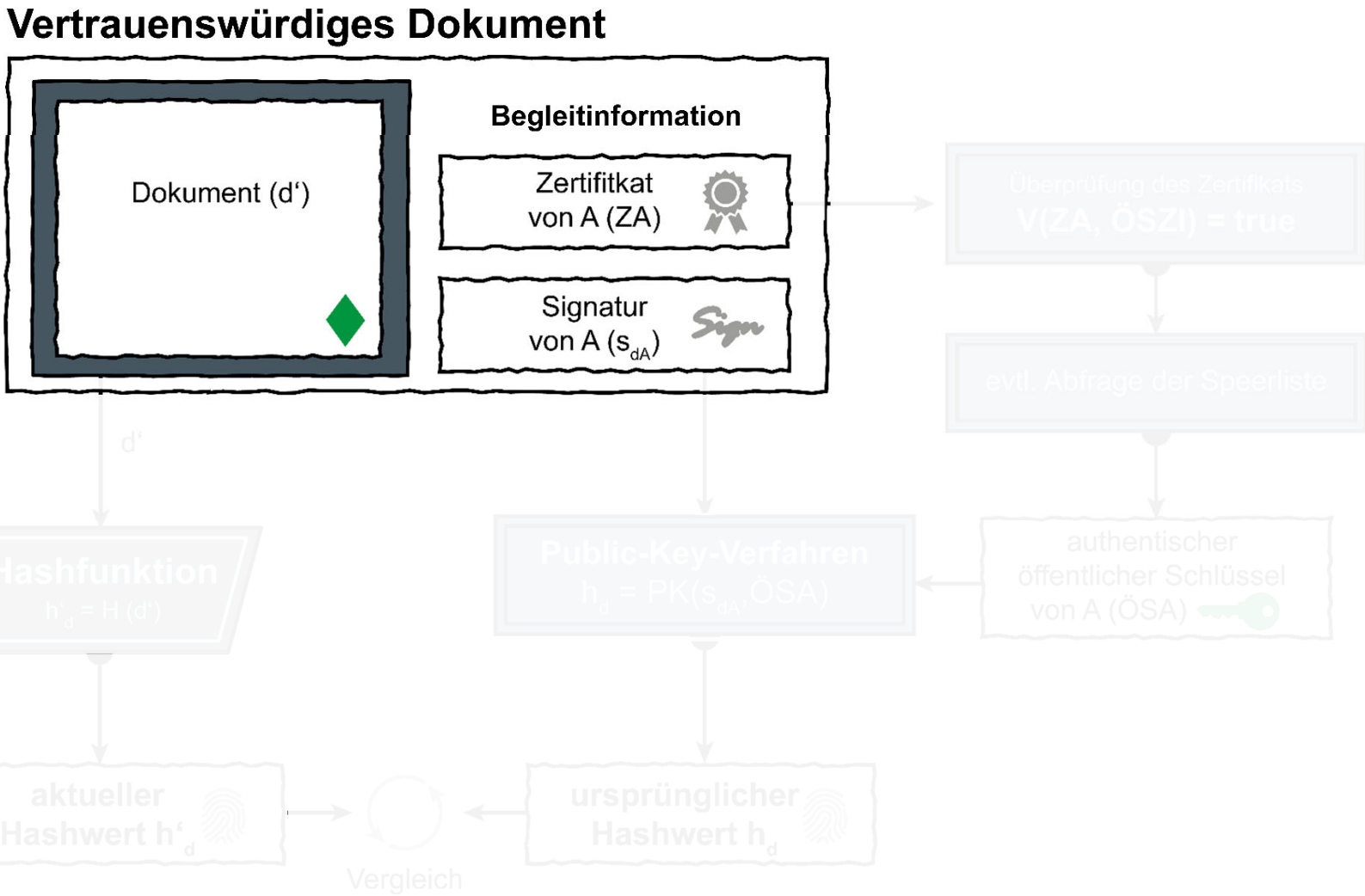
PKI-enabled Application
→ E-Mail Sicherheit (5/8)



PKI-enabled Application
→ E-Mail Sicherheit (6/8)



PKI-enabled Application
→ E-Mail Sicherheit (6/8)



PKI-enabled Application
→ E-Mail Sicherheit (7/8)

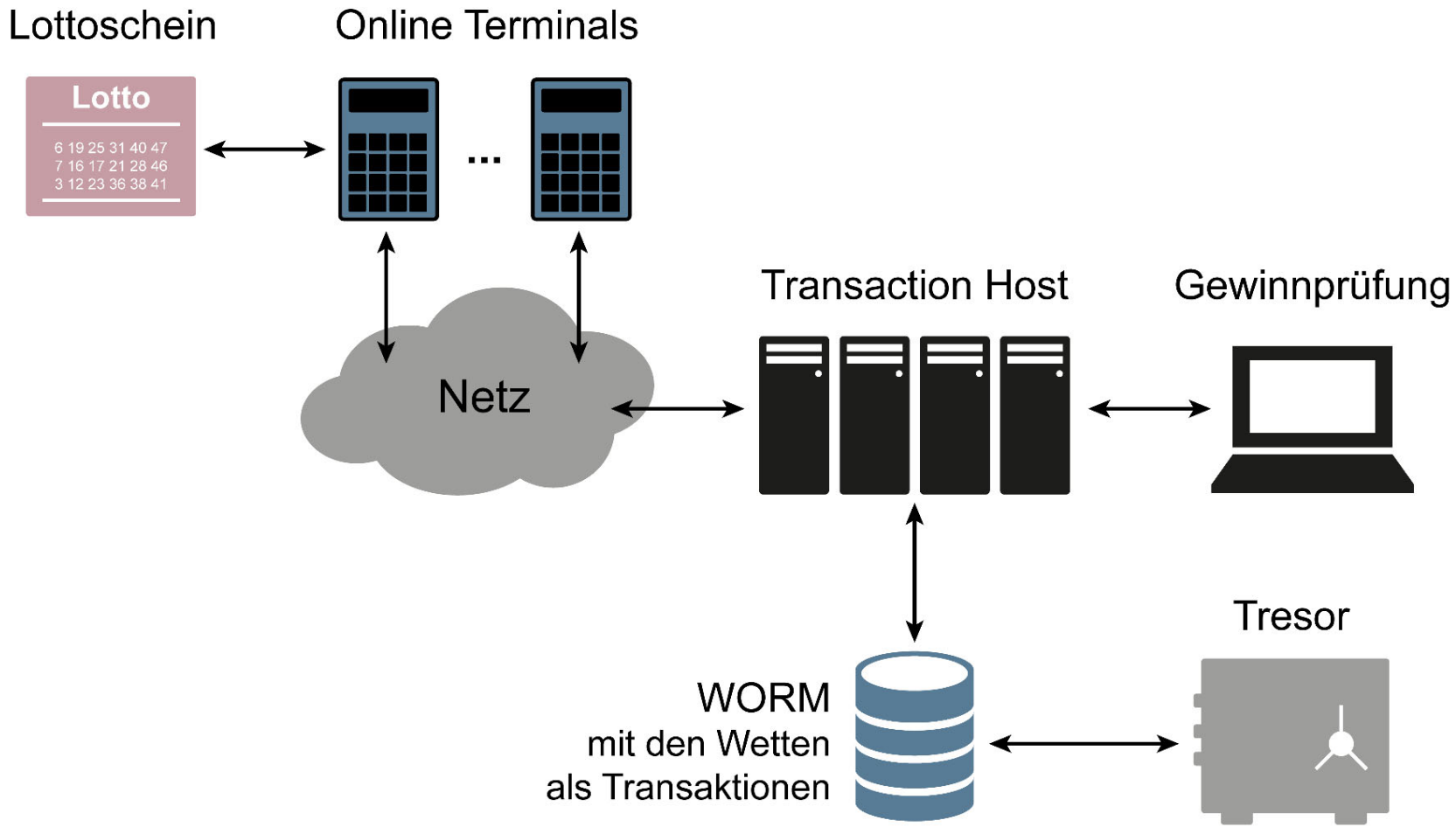
- Nach erfolgreicher Überprüfung der Signatur ist sichergestellt, dass das Dokument **unversehrt** übertragen worden ist. Das bedeutet:
  - Niemand hat das Dokument manipuliert (Gewährleistung der **Datenunversehrtheit**).
  - Die angegebene Zeit der Signatur wurde nicht geändert.
  - Nur die Nutzer, die in den Begleitinformationen angegeben sind, konnten die entsprechende Signatur durchführen.
- Diese Funktionen machen die digitale Signatur zum elektronischen Äquivalent der eigenhändigen Unterschrift.
- Als zusätzliche Sicherheitsfunktion steht die Verschlüsselung des Dokuments zur Verfügung, die seine Vertraulichkeit garantiert.

PKI-enabled Application
→ E-Mail Sicherheit (8/8)

- E-Mail-Sicherheit aus Sicht des Nutzers?
- Die Sicherheitsfunktionen werden in die Anwendungen integriert (z.B. Mailsoftware und Browser).
- Der Nutzer kann dabei durch einfachen Mausklick die Sicherheitsfunktionen aufrufen.
- Je einfacher die Nutzbarkeit der Sicherheitsfunktionen ist, desto höher wird die Akzeptanz der Nutzer sein.
- E-Mail-Gateways können eingehende E-Mails zentral entschlüsseln und intern verteilen, oder ausgehende E-Mails signieren.
  - Empfänger kann sicher sein, dass diese Mails wirklich von der entsprechenden Organisation stammen.

PKI-enabled Application
→ Lotto–Online-Glückspiel (1/4)

- Altes Verfahren der Manipulationssicherung von Wetten:



PKI-enabled Application
→ Lotto–Online-Glückspiel (1/4)

- Altes Verfahren der Manipulationssicherung von Wetten:

PKI-enabled Application
→ Lotto–Online-Glückspiel (2/4)

- Neue Herausforderungen: Gewinnspiele (z.B: Sportwetten) mit sehr viel schnelleren Lebenszyklen.

- Ablösung des WORM durch Nutzung eines Zeitstempeldienstes für Manipulationssicherung von Transaktionsdaten.

$$h = H\ (Transaction, Datum, Uhrzeit)$$

- Anschließend wird dann dieser Hashwert mit dem geheimen Schlüssel von Lotto (GS_{Lotto}) digital signiert.

$$s = S\ (h, GS_{Lotto})$$

PKI-enabled Application
→ Lotto–Online-Glückspiel (3/4)

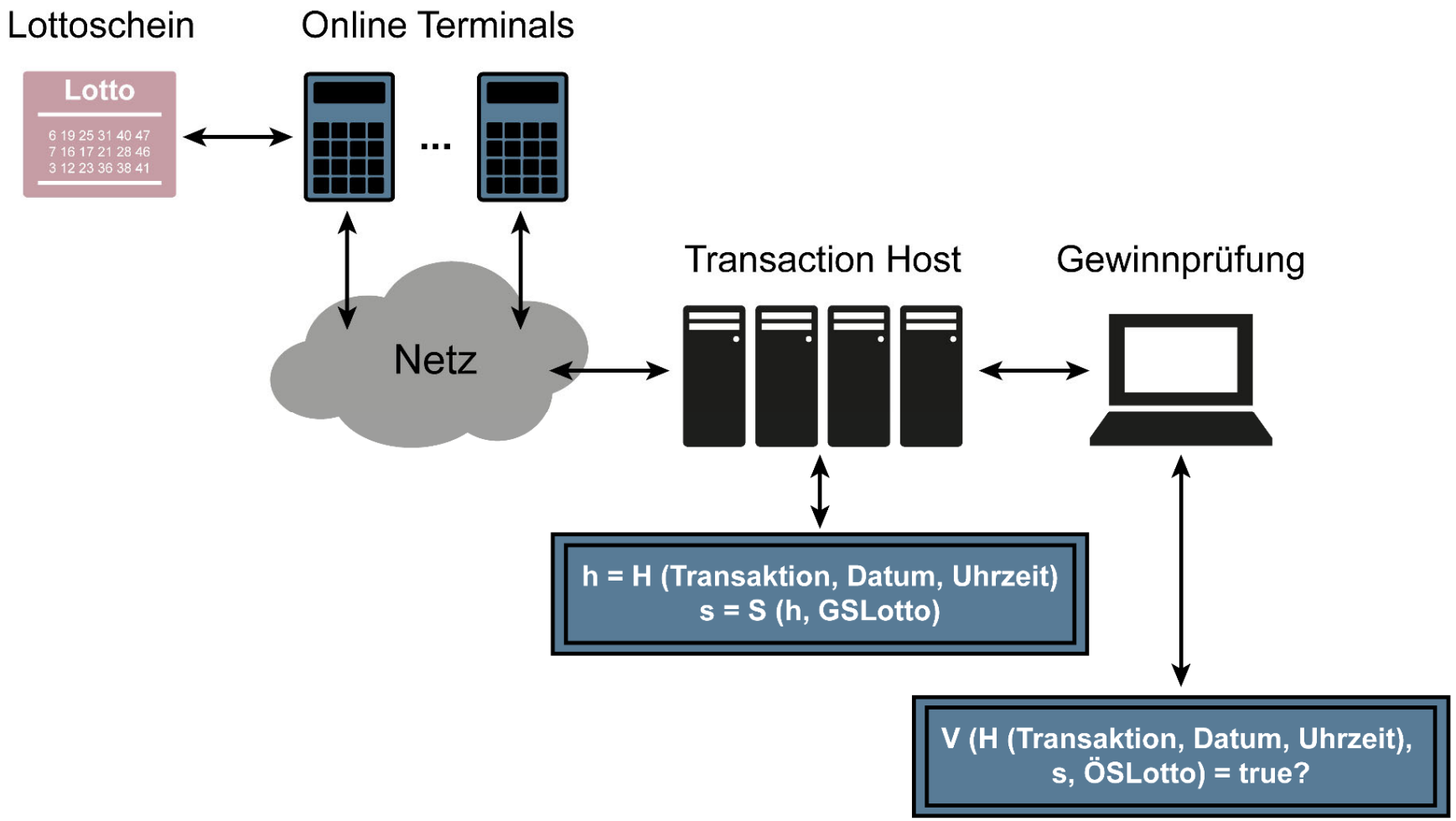
- Wenn die Ziehung vorbei ist, kann die Gewinnprüfung umgesetzt und jede Transaktion verifiziert werden.

$V\ (H\ (\text{Transaktion, Datum, Uhrzeit}),\ s,\ OS_{Lotto}) = \text{true?}$

V: Verifikationsfunktion
H: Hashfunktion
S: Signaturfunktion
s: Signatur der Transaktion
OS_{Lotto} : Öffentlicher Schlüssel von Lotto

PKI-enabled Application
→ Lotto–Online-Glückspiel (4/4)

- Neus Verfahren der Manipulationssicherung von Wetten:



PKI-enabled Application
→ Lotto–Online-Glückspiel (4/4)

- Neus Verfahren der Manipulationssicherung von Wetten:

Signatur, Zertifikate und PKI
→ Inhalt

- Ziele und Ergebnisse der Vorlesung
- Digitale Signaturen und Zertifikate
- Public-Key-Infrastrukturen
- Gesetzlicher Hintergrund
- PKI-enabled Application
- **Zusammenfassung**

Signatur, Zertifikate und PKI
→ Zusammenfassung

- Digitale Signatur, elektronische Zertifikate und Public-Key-Infrastrukturen sind wichtige Cyber-Sicherheit-Prinzipien, -Mechanismen und -Konzepte für die Realisierung von Cyber-Sicherheitslösungen und -Diensten.

- Public-Key-Infrastrukturen stellen die Basis für organisationsübergreifende Cyber-Sicherheitssysteme dar und haben über eIDAS in Europa eine rechtliche Grundlage.

- Die Beispiele der PKI-enabled Application zeigen auf, was mit den Vertrauensdiensten einer PKI an sicherheitsrelevante Anwendungen umgesetzt werden können.

Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Signatur, Zertifikate und PKI

- Vorlesung Cyber-Sicherheit -

Prof. Dr. (TU NN)
Norbert Pohlmann

Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen
http://www.internet-sicherheit.de

if(is) internet-sicherheit.

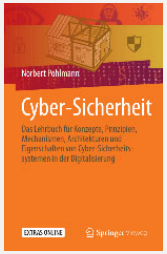
Anhang / Credits

Wir empfehlen

- **Kostenlose App securityNews**

securityNews

- **7. Sinn im Internet (Cyberschutzraum)**
  https://www.youtube.com/cyberschutzraum
- **Master Internet-Sicherheit**
  https://it-sicherheit.de/master-studieren/
- **Cyber-Sicherheit**
  Das **Lehrbuch** für Konzepte, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung“, Springer Vieweg Verlag, Wiesbaden 2019
- https://norbert-pohlmann.com/cyber-sicherheit/



Besuchen und abonnieren Sie uns :-)

WWW
https://www.internet-sicherheit.de

Facebook
https://www.facebook.com/Internet.Sicherheit.ifis

Twitter
https://twitter.com/_ifis

YouTube
https://www.youtube.com/user/InternetSicherheitDE/

Prof. Norbert Pohlmann
https://norbert-pohlmann.com/

Quellen Bildmaterial

Eingebettete Piktogramme:
- Institut für Internet-Sicherheit – if(is)

Der Marktplatz IT-Sicherheit

(IT-Sicherheits-) Anbieter, Lösungen, Jobs, Veranstaltungen und Hilfestellungen (Ratgeber, IT-Sicherheitstipps, Glossar, u.v.m.) leicht & einfach finden.
https://www.it-sicherheit.de/

Literatur
→ Artikel / Bücher

M. Hesse, N. Pohlmann: „Kryptographie: Von der Geheimwissenschaft zur alltäglichen Nutzanwendung (VI) – Public Key Infrastruktur (PKI)“, IT-Sicherheit & Datenschutz, Supplement in DuD Datenschutz und Datensicherheit - Recht und Sicherheit in Informationsverarbeitung und Kommunikation, Vieweg Verlag, 04/2007
https://norbert-pohlmann.com/wp-content/uploads/2015/08/196-Kryptographie-Von-der-Geheimwissenschaft-zur-alltäglichen-Nutzanwendung-VI-–-Public-Key-Infrastruktur-PKI-Prof.-Norbert-Pohlmann.pdf

M. Hertlein, P. Manaras, N. Pohlmann: „Smart Authentication, Identification and Digital Signatures as Foundation for the Next Generation of Eco Systems”, In the Book ”Digital Marketplaces Unleashed”, Editors: Claudia Linnhoff-Popien, Ralf Schneider and Michael Zaddach, Springer-Verlag GmbH Germany, 2017
https://norbert-pohlmann.com/wp-content/uploads/2019/07/362-Smart-Authentication-Identification-and-Digital-Signatures-as-Foundation-for-the-Next-Generation-of-Eco-Systems-Prof.-Norbert-Pohlmann.pdf

N. Pohlmann: "Firewall-Systeme - Sicherheit für Internet und Intranet, E-Mail-Security, Virtual Private Network, Intrusion Detection System, Personal Firewalls“, 5. aktualisierte und erweiterte Auflage, 604 Seiten, MITP-Verlag, Bonn 2003
http://norbert-pohlmann.com/app/uploads/2015/08/Firewall-Systeme.pdf

H. Blumberg, N. Pohlmann: "Der IT-Sicherheitsleitfaden“, 2. aktualisierte und erweiterte Auflage, 523 Seiten, MITP-Verlag, Bonn 2006
https://norbert-pohlmann.com/wp-content/uploads/2019/08/IT-Sicherheitsleitfaden-Prof.-Norbert-Pohlmann.pdf

N. Pohlmann: "Cyber-Sicherheit – Das Lehrbuch für Konzepte, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung“, ISBN 978-3-658-25397-4; 594 Seiten, Springer-Vieweg Verlag, Wiesbaden 2019
https://norbert-pohlmann.com/cyber-sicherheit/