

Freitag, 03.03.2006
IT Security Day



Sicherheit im Bereich der Finanzdienstleistungen



Sicherheit im Bereich der Finanzdienstleistungen



Inhalt



Datensicherheit im Allgemeinen

- Datensicherheit (Schutz vor Verlust, Backup, Disaster Recovery)
- Datenschutz (Schutz vor Diebstahl, Manipulation)

Das Bancomatsystem

- Was ist Standard?
- Was ist möglich?
- Wie kann ich mich schützen?

Inhalt



Online Kreditkartenzahlungen

- Wer trägt welches Risiko?
- VPOS (Verschlüsselung der Kartendaten)
- Bankpass (virtueller PAN)
- Verified by Visa (Authentifizierung des Kunden)

Online Banking

- Systemsicherheit (Server, Netz, SSL)
- Anwendersicherheit (Umgang mit Passwörter, SPAM ermöglicht Phishing)
- Anwendungssicherheit (Programmierung, SQL-injection, XSS)

Schutz der eigenen Firma → Schutz der eigenen Daten



Allgemein

- Datenverlust (wie hoch ist der Aufwand, meine Daten zu reproduzieren?)
- Systemausfall (was kostet mich der Tag/Stunde/Minute)

Im Netz

- Vertraulichkeit (Verschlüsselung)
- Nicht Abstreitigkeit (non repudiation)
- Integrität (Veränderung, Verlust, Wiederholung)
- Authentifizierung (wer ist wer)
- Autorisierung (wer darf was)

Sicherheit im Netz (Daten -Vertraulichkeit)



Kunde

Meine Kreditkartennummer
ist X fällig am 31.12.98



Bank

OK, Auftrag erhalten,
Belastung durchgeführt

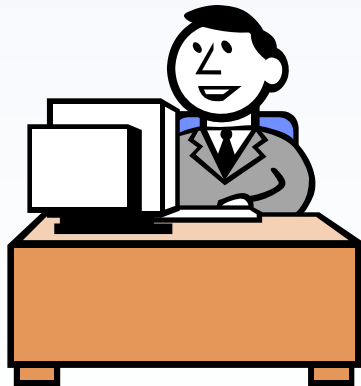


Sicherheit im Netz (Daten -Integrität/Verlust)



Kunde

Überweisen Sie 1.000 € auf
das Konto 12345

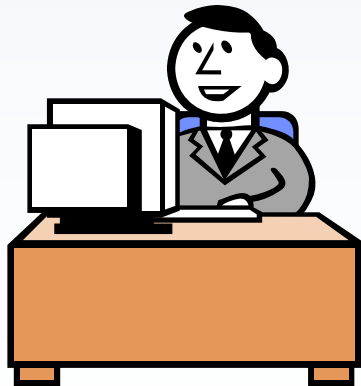


Sicherheit im Netz (Daten - Integrität/Änderung)



Kunde

Überweisen Sie 1.000 € auf
das Konto 12345



Überweisen Sie 10.000 €
auf das Konto 54321

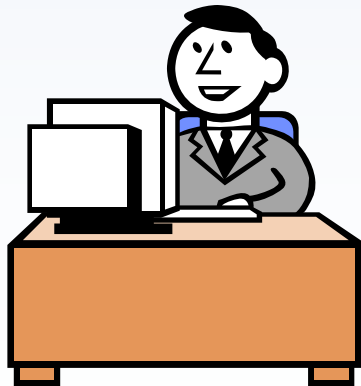


Sicherheit im Netz (Daten - Wiederholung)



Kunde

Überweisen Sie 1.000 €



Bank

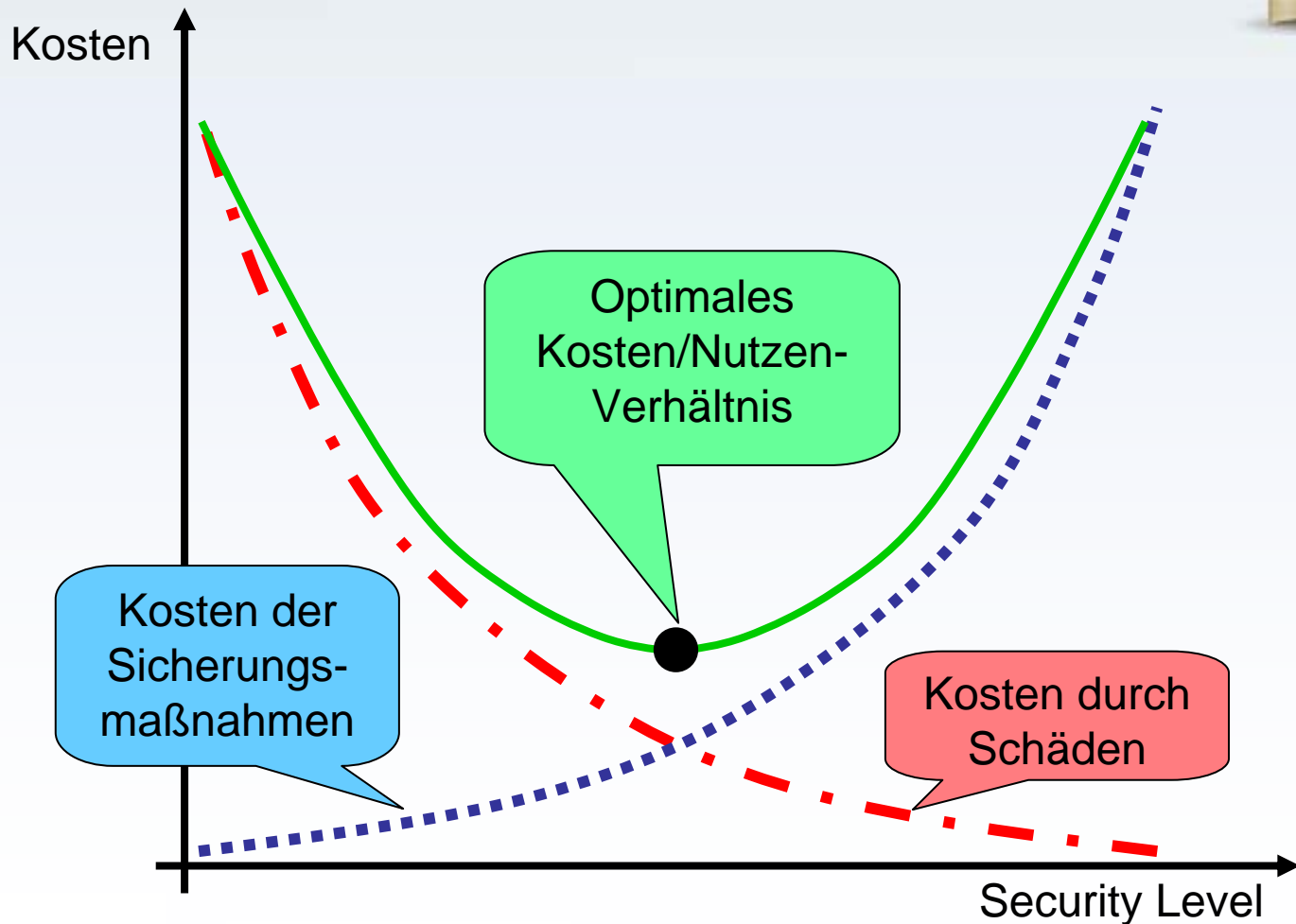
Überweisen Sie 1.000 €

Überweisen Sie 1.000 €

Überweisen Sie 1.000 €



"angemessene" Sicherheitsmaßnahmen



Maßnahmen

Integrität durch Checksumme



Daten: 111111
Übertr.: 1111116



$6 = f(111111)$

z.B. $1 + 1 + 1 + 1 + 1 + 1$

Maßnahmen symmetrische Verschlüsselung

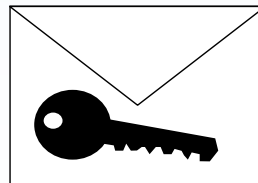


AX678yUz.ki@...



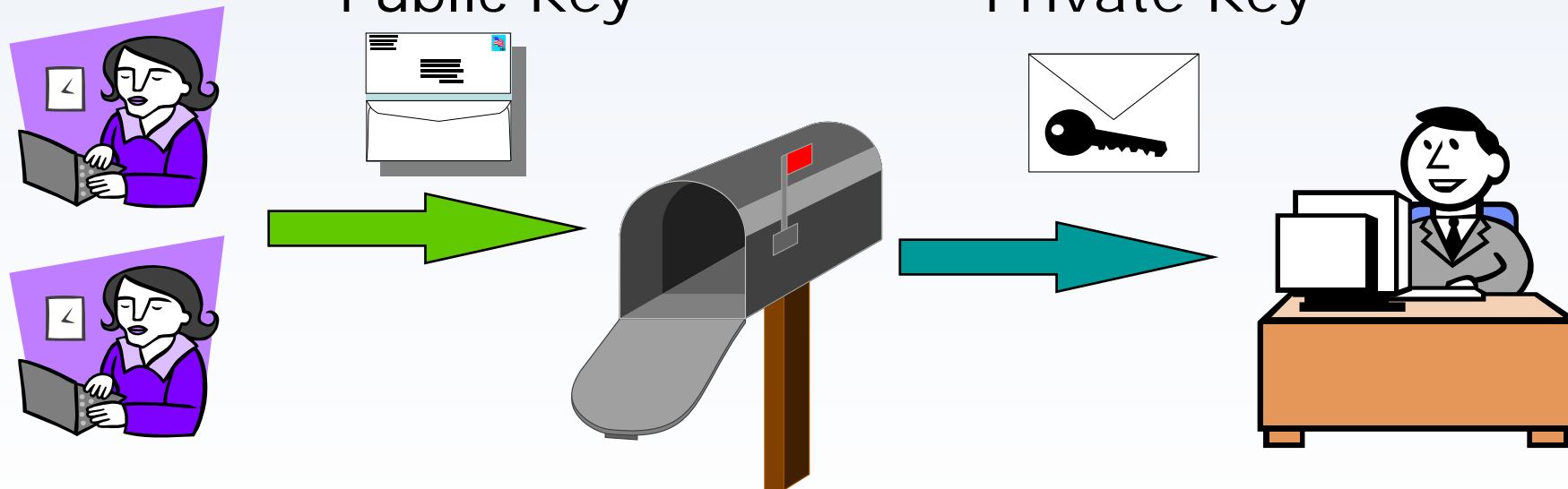
111111

+ 4

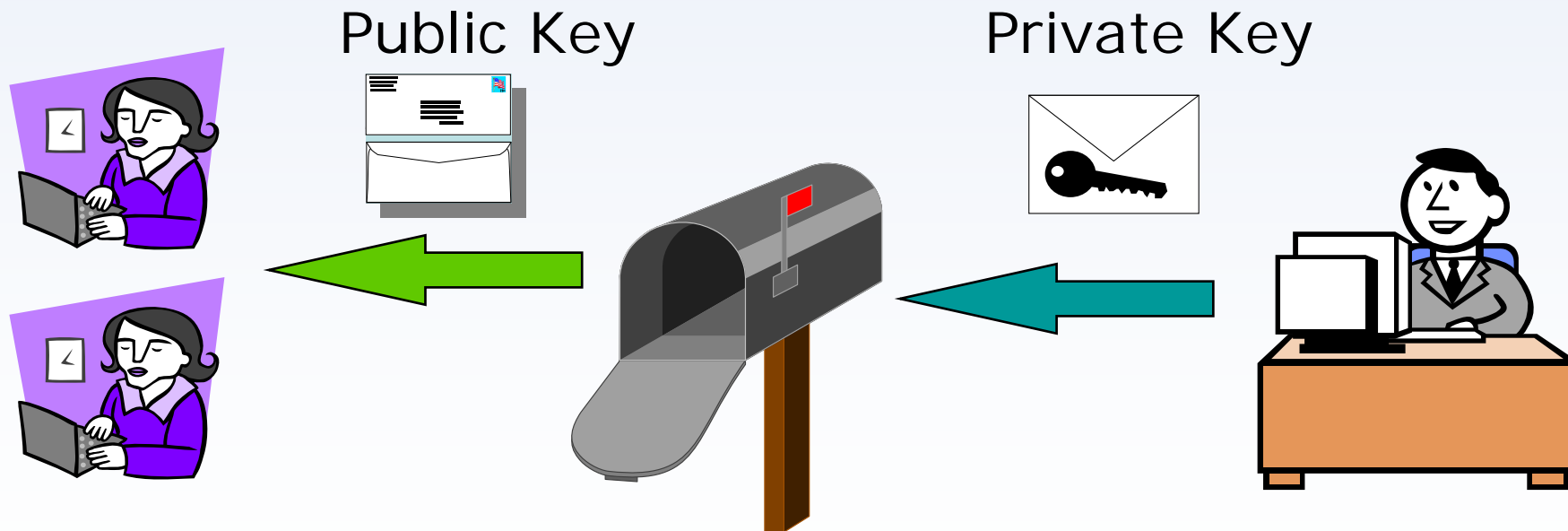


555555

Maßnahmen asymmetrische Verschlüsselung



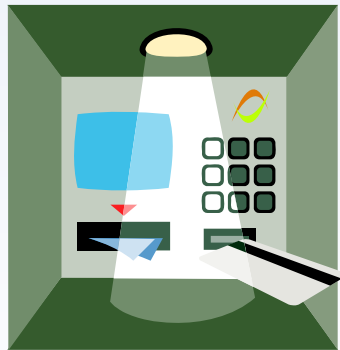
Vertraulichkeit durch asymmetrische Verschlüsselung



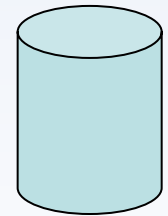
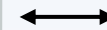
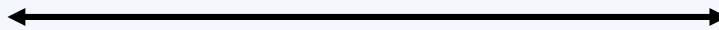
Bancomat/POS



Bancomatbehebung im Inland



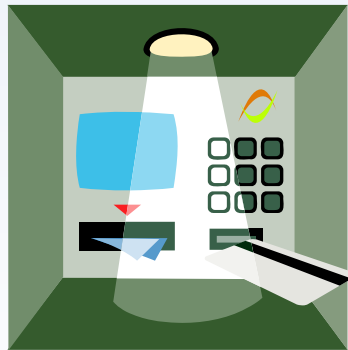
**Daten werden online zentral
überprüft und Magnetspur mit
Sicherheitsinformationen
überschrieben**



**Magnetspur wird gelesen und
der PIN abgefragt**

**Sicherheitsmerkmale (u.aA. Random)
wird in DB gespeichert und muss
der der nächsten Behebung
übereinstimmen.
Zudem update der Tages/Monatslimits**

Bancomatbehebung im Ausland

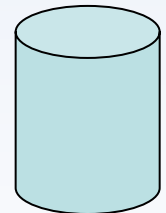


Magnetspur wird gelesen und der PIN abgefragt (errechnet)

Daten werden online zentral überprüft



Clearingstelle



Die Tages- und Monatslimits werden überprüft und aktualisiert

Sicherheit bei den Kartensystemen



Internationale Produkte

- Cirrus/Maestro

- PIN Kontrolle nur am Bancomat
- Am POS nur langsame Umstellung von Unterschrift auf PIN
- Teils - Offline Zahlungen möglich
- Keine besonderen Sicherheitsmerkmale auf der Spur

- Kreditkarten

- PIN Kontrolle nur am Bancomat, wenn überhaupt, möglich
- Am POS nach wie vor nur mit Unterschrift
- Magnetspur ohne Sicherheitsmerkmale
- Zahlungen ohne Karte möglich !!
- Zum Teil immer noch Offlinezahlungen möglich

Sicherheit bei den Kartensystemen



Schadensfälle

- Größtenteils durch **Duplizierung** der Karte
 - Am Bancomat → zweites Lesegerät und Videokamera
 - Am POS → Austausch des Gerätes wobei das „neue“ Gerät intern verändert wurde.
- und Behebung im **Ausland**,
- am besten übers Wochenende bzw. am Monatsende.

Verlust/Diebstahl/Klonen



- 🔒 Verlust der Karte ohne PIN
 - Inland kein Problem (höchstens Fastpay)
 - Ausland (je nach Land wird nur die Unterschrift kontrolliert - signature based)
- 🔒 Verlust der Karte mit PIN
 - Problem bis zur Sperrung
- 🔒 Klonen der Karte ohne PIN
 - Inland kein Problem (höchstens Fastpay)
 - Ausland (je nach Land wird nur die Unterschrift kontrolliert)
- 🔒 Klonen der Karte mit PIN
 - im Inland kaum Probleme (wegen der Random Nr., Ausnahme POS)
 - im Ausland Behebung innerhalb es Limits
 - im Ausland Behebung über Monatsende

Sicherheit bei den Kartensystemen



Maßnahmen

- am Bancomat
 - Gezielte Hinweisschilder
 - Vorrichtungen die das "klonen" der Karte unterbinden
 - Anpassungen, die das manipulieren des Gerätes verhindern
- am POS
 - POS Betreiber auf Risiken hinweisen
 - EMV fähige Geräte installieren
- Karte
 - EMV Umstellung vorantreiben

Sicherheit bei den Kartensystemen



weitere Maßnahmen

- Eine einzige Autorisierungsstelle (die eigene Bank)
- Monitoring / Überwachung der Operationen
- Plausibilitätsprüfungen erstellen
- SMS Dienst bei verdächtigen Operationen (bzw. Ausland)
- Sehr wirksam wäre ein "numero Random" auf der Auslandsspur, allerdings aufwendig und schwierig zu realisieren.

Die Zukunft?



- 🔒 Magnetspur wird durch Chip ersetzt (kopiersicher)
- 🔒 Lesegeräte am Bancomaten werden ausgetauscht
- 🔒 POS-Geräte müssen ausgetauscht werden
- 🔒 Ausland:
 - hat bereits viele Karten ersetzt
 - hinkt aber mit den Geräten hinterher
 - de Facto wird noch die Magnetspur verwendet
 - Fazit: solange Magnetspur verwendet wird ist der Sicherheitsstandard geringer als in Italien

Online Kreditkartenzahlungen



Online Kreditkartenzahlungen



- 🔒 Wie übermittle ich meine Kreditkartennummer (SSL)
- 🔒 Wer ist der Empfänger
- 🔒 Wie sicher ist das Informationssystem des Empfängers
- 🔒 Solange keine Unterschrift vorliegt, hat der Kunde "Recht"
- 🔒 Ehrliche Händler können "geprellt" werden

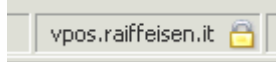
Verschlüsselung der Daten



Im IE:



Im Firefox:



Der Klick
auf
Nummer sicher!



Name

E-Mail

Kreditkartennummer

Sicherheitscode

Fälligkeit 01 2006

Kreditkarte American Express

Betrag 1.00 EUR



Sicherheit:

Sie haben soeben einen geschützten Bereich betreten. Die Datenübermittlung von und zum Server wird zu Ihrer Sicherheit durch SSL vor unautorisiertem Zugriff geschützt.



Seiteninformation

Allgemein | Formulare | Links | Medien | Sicherheit

Website-Identität verifiziert

Die Website vpos.raiffeisen.it unterstützt Authentifizierung für die Seite, die Sie ansehen. Die Identität dieser Website wurde verifiziert von Thawte Consulting (Pty) Ltd., einer Zertifizierungsstelle, der Sie für diesen Zweck vertrauen.

Sicherheitszertifikate anzeigen, die die Identität dieser Website verifizieren.

Verbindung verschlüsselt: Verschlüsselung auf hoher Stufe (AES-256 256 bit)

Die Seite, die Sie anzeigen, wurde verschlüsselt, bevor sie über das Internet übermittelt wurde. Verschlüsselung macht es sehr schwierig für unberechtigte Personen, zwischen Computern übertragene Informationen auszuspähen. Daher ist es sehr unwahrscheinlich, dass jemand diese Seite gelesen hat, als sie durch das Netzwerk geschickt wurde.



Kundenschutz



Bankpass (Wegwerfkreditkarte)

- Kunde erhält Zugriff wie bei Online Banking auf Seite der SSB (Società per i Servizi Bancari)
- Kunde kann sich dort eine Wegwerfkreditkartennummer "erzeugen" lassen
- diese Kreditkartennummer kann nur 1 x für max. den explizit angegebenen Betrag verwendet werden
- nach der Zahlung ist die Karte nicht mehr gültig
- logische Verknüpfung zwischen virtueller und physischer Kreditkarte

Bankpass - virtuale Kreditkarte



Raiffeisen

Salve **EDMUND SCHOEPP** sei nella home page della tua area privata

ANTEPRIMA RENDICONTAZIONE

Data	Esercente	n° ordine	Importo	Valuta
------	-----------	-----------	---------	--------

RENDICONTAZIONE COMPLETA **PAN GENERATI**

[Esci](#)

[Modifica il tuo profilo](#)

[Gestisci il tuo wallet](#)

Crea PAN virtuale

User ID

Password

CREA

Si Servizi **info** **BANKPASS Web**

Bankpass - virtuelle Kreditkarte



Raiffeisen

Creazione PAN virtuale

** I Campi contrassegnati con asterisco sono Obbligatori*

Importo dell'acquisto* , euro

Generail PAN con*

Promemoria (massimo 50 caratteri)

E-Mail: **edmund.schoepf@raiffeisen.it**

[VAI ALLA TUA HOME PAGE](#) [CONFERMA](#)



Bankpass - virtuelle Kreditkarte



Importo dell'acquisto **103,50** Valuta **EUR**

Data **02/02/2006** Ora **14:06**

Hai generato il PAN virtuale con:
CartaSi Master - MASTERCARD - SI

Promemoria acquisto:
Ankauf Software aus RUSSLAND

E-mail: **edmund.schoepf@raiffeisen.it**

I dati per l'acquisto, da inserire sul sito del tuo esercente, sono:

Pan virtuale 51 566
Data scadenza 03-06 (mm/aa)
cvv2 500

[VAI ALLA TUA HOME PAGE](#) [CHIUDI](#) [STAMPA](#)



Bankpass - virtuelle Kreditkarte



 **Raiffeisen** Meine Bank

[Hilfe](#) | [Info](#)



Der Klick
auf
Nummer sicher!


CaravanPark Sesto
Adventures
in the Dolomites

Name	<input type="text" value="Edmund"/>
E-Mail	<input type="text" value="edmund.schoepf@raiffeisen.it"/>
Kreditkartennummer	<input type="text" value="500222233334444"/>
Sicherheitscode	<input type="text" value="774"/>
Fälligkeit	<input type="text" value="01"/> <input type="text" value="2006"/>
Kreditkarte	<input type="text" value="Mastercard"/>
Betrag	11.00 EUR

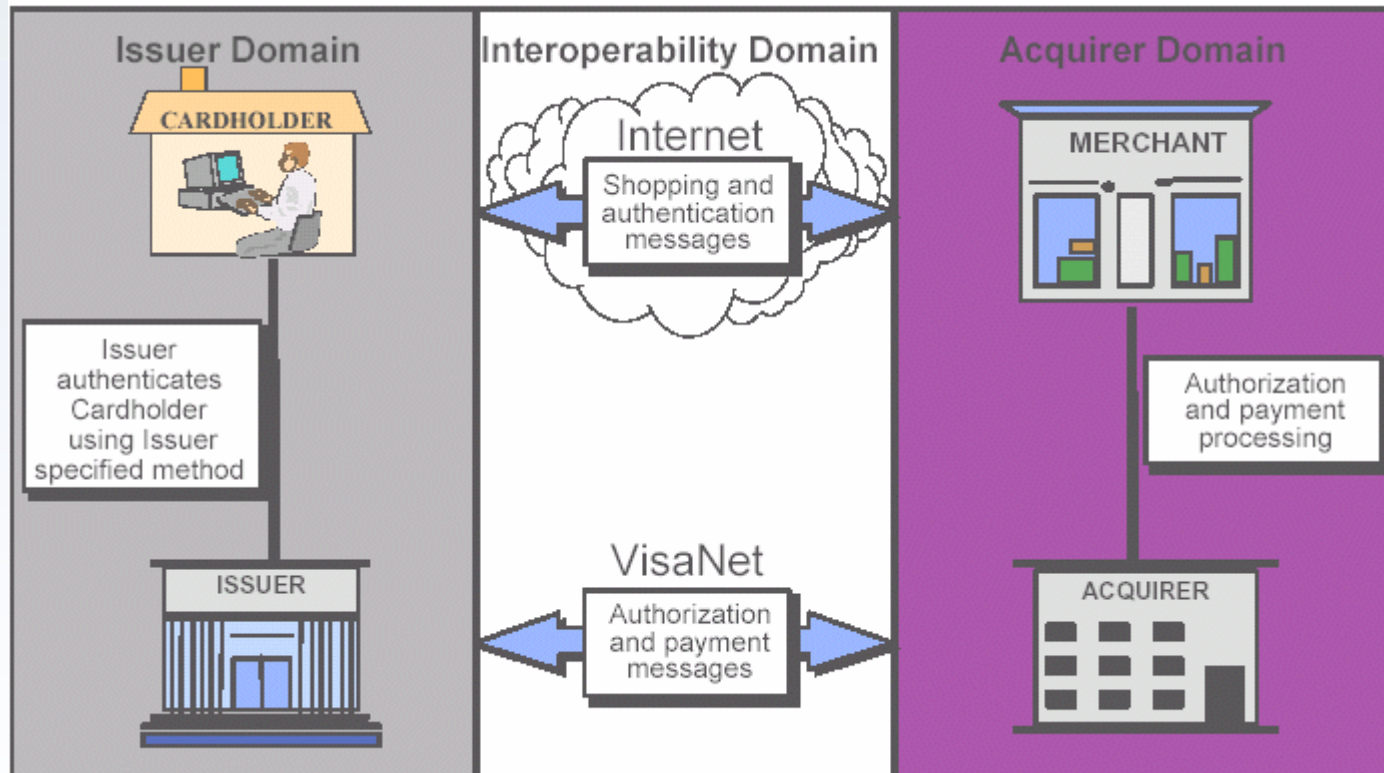


Sicherheit:

Sie haben soeben einen geschützten Bereich betreten. Die Datenübermittlung von und zum Server wird zu Ihrer Sicherheit durch SSL vor unauthorisiertem Zugriff geschützt.



Händlerschutz



Händlerschutz

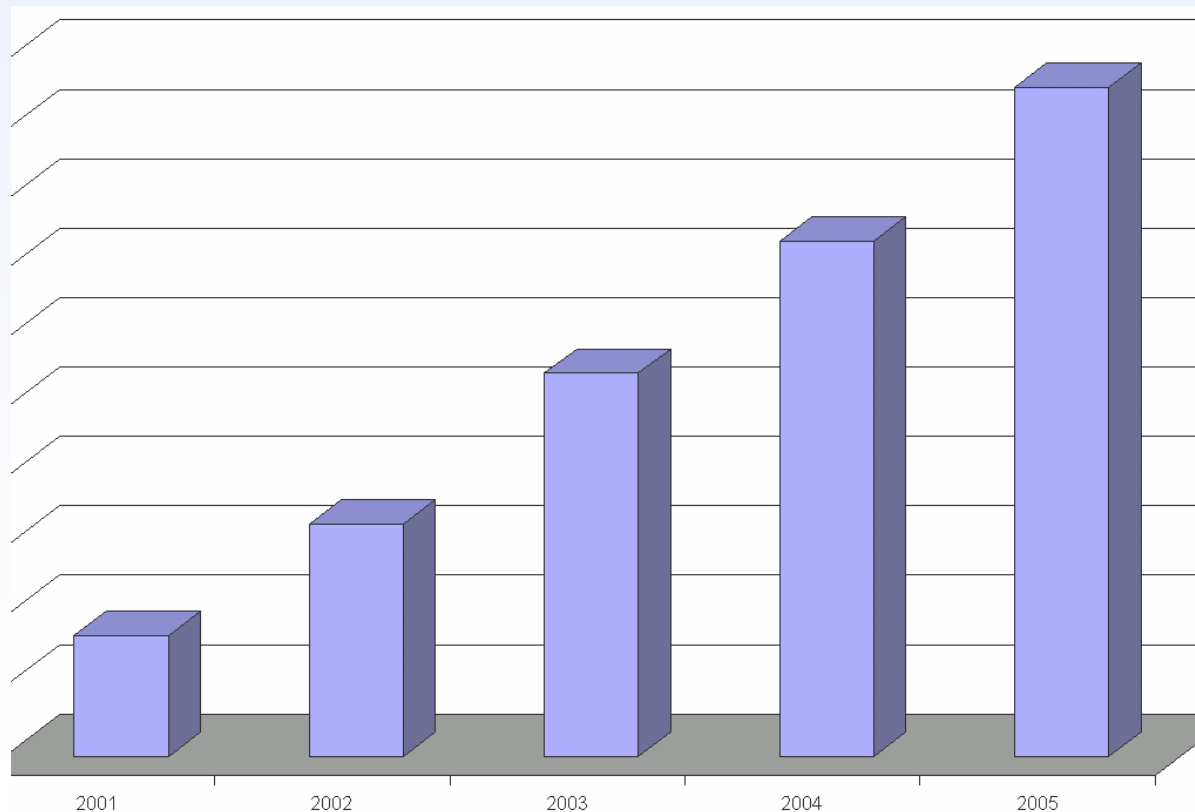


- 🔒 Verified By Visa/Mastercard Secure Code
 - Kreditkartenkunde ist bei seiner Bank registriert
 - tätigt Online Einkauf und
 - gibt seine Kreditkartennummer ein
 - bevor diese überprüft werden kann
 - muss der Kunde sein Password eingeben
 - somit weiß der Shopbetreiber, dass der Kunde der Besitzer der Kreditkarte ist

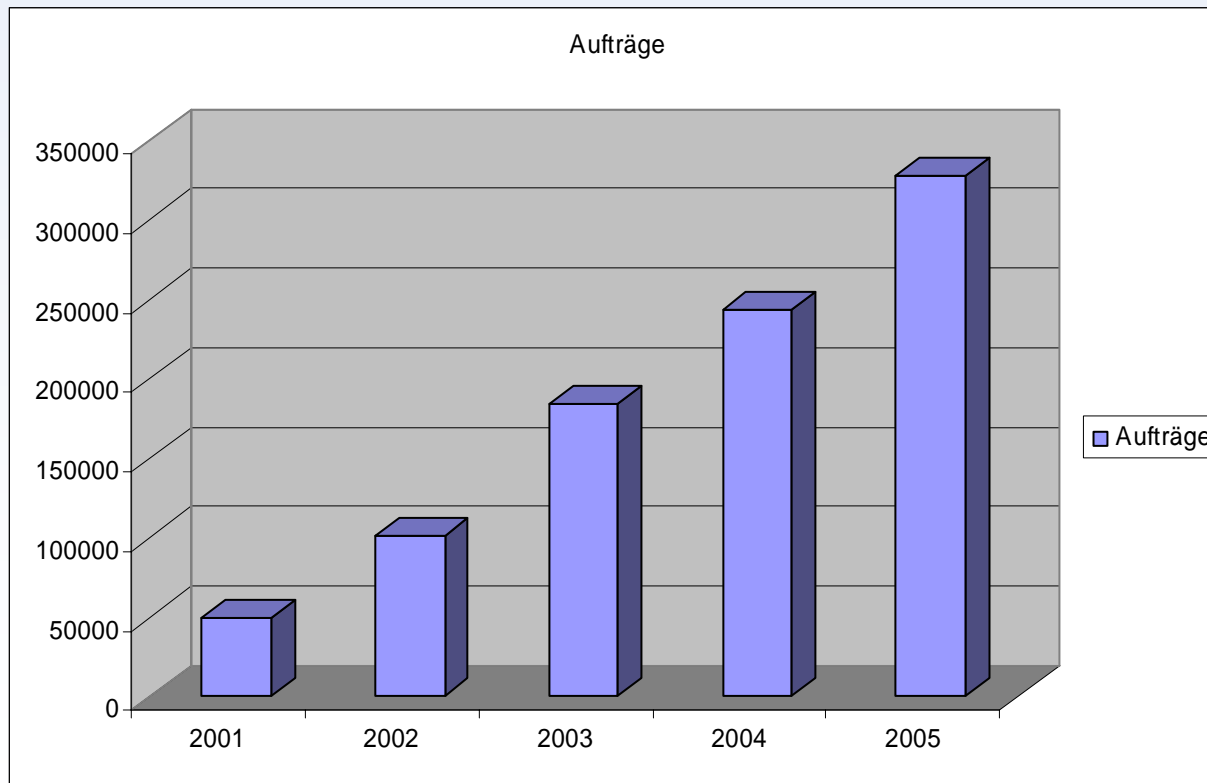
Online Banking



Anzahl der Benutzer, die online Aufträge erteilen (5 x)



Online Aufträge (10 x seit 2001)

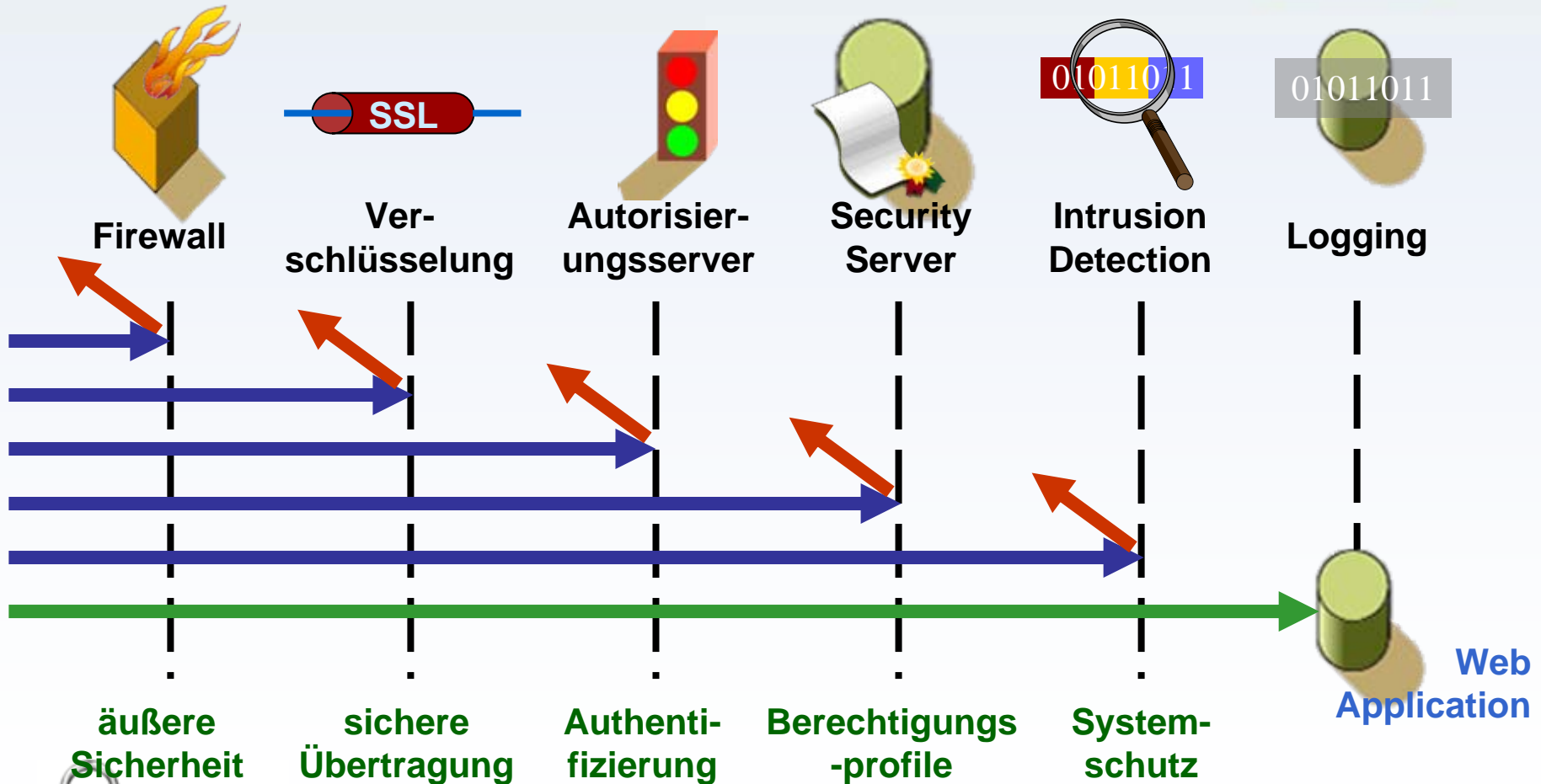


Sicherheit beim Online Banking



- 🔒 Systemsicherheit (aktuelle gepatchte Server)
- 🔒 Netzwerksicherheit (Firewalls, IDS)
- 🔒 Datensicherheit (Backups)
- 🔒 Datenschutz (Verschlüsselung)
- 🔒 Authentifizierung (wer ist wer?)
- 🔒 Autorisierung (wer darf was?)
- 🔒 Anwendungssicherheit

Netzwerkulnerabilität



Top 10 Schwachstellen einer Anwendung



OWASP Top Ten Most Critical Web Application Security Vulnerabilities		
<u>A1</u>	Unvalidated Input	Information from web requests is not validated before being used by a web application. Attackers can use these flaws to attack backend components through a web application.
<u>A2</u>	Broken Access Control	Restrictions on what authenticated users are allowed to do are not properly enforced. Attackers can exploit these flaws to access other users' accounts, view sensitive files, or use unauthorized functions.
<u>A3</u>	Broken Authentication and Session Management	Account credentials and session tokens are not properly protected. Attackers that can compromise passwords, keys, session cookies, or other tokens can defeat authentication restrictions and assume other users' identities.
<u>A4</u>	Cross Site Scripting (XSS) Flaws	The web application can be used as a mechanism to transport an attack to an end user's browser. A successful attack can disclose the end user's session token, attack the local machine, or spoof content to fool the user.
<u>A5</u>	Buffer Overflows	Web application components in some languages that do not properly validate input can be crashed and, in some cases, used to take control of a process. These components can include CGI, libraries, drivers, and web application server components.
<u>A6</u>	Injection Flaws	Web applications pass parameters when they access external systems or the local operating system. If an attacker can embed malicious commands in these parameters, the external system may execute those commands on behalf of the web application.
<u>A7</u>	Improper Error Handling	Error conditions that occur during normal operation are not handled properly. If an attacker can cause errors to occur that the web application does not handle, they can gain detailed system information, deny service, cause security mechanisms to fail, or crash the server.
<u>A8</u>	Insecure Storage	Web applications frequently use cryptographic functions to protect information and credentials. These functions and the code to integrate them have proven difficult to code properly, frequently resulting in weak protection.
<u>A9</u>	Denial of Service	Attackers can consume web application resources to a point where other legitimate users can no longer access or use the application. Attackers can also lock users out of their accounts or even cause the entire application to fail.
<u>A10</u>	Insecure Configuration Management	Having a strong server configuration standard is critical to a secure web application. These servers have many configuration options that affect security and are not secure out of the box.

Online Banking - verschiedene Sicherheitssysteme



- 🔒 User und Passwort
- 🔒 TAN (Transaktions Nummer)
- 🔒 Kreuztabelle
- 🔒 Zufallsfragen
- 🔒 Informationen Lokal auf PC
- 🔒 One Time Code/One Time Passwort
- 🔒 Zertifikat (für Authentifizierung und digitale Signatur)

Online Banking



- 🔒 Vorsicht im Umgang mit den persönlichen Daten (Phishing - Password Fishing):
 - User
 - Passwort
- 🔒 von wo aus verbinde ich mich mit der Bank
 - zu Hause
 - Arbeitsplatz
 - Internetkaffee
- 🔒 wie geschützt ist mein PC / Verbindung

Verhaltensregeln (2)



- 🔒 **Wechseln Sie Ihr Passwort regelmäßig!**
 - Durch das regelmäßige Ändern beschränken Sie
 - zeitlich die Möglichkeit eines Hackers im Falle
- 🔒 **eines kompromittierten Passworts.**
 - Verwenden Sie verschiedene Passwörter für verschiedene Systeme!
 - Ein potentieller Angreifer ist dadurch eingeschränkt.
- 🔒 **Achtung im Internet!**

Anforderungen an ein Passwort (1)



Vermeiden sollte man

- Wörter oder einfache Abkürzungen, die im Wörterbuch zu finden sind.
- Eigennamen oder persönliche Daten wie Geburtstag, Autokennzeichen, etc.
- Einfach rückwärts geschriebene Wörter
- Passwörter mit großen Buchstaben nur am Anfang
- Passwörter mit Sonderzeichen nur am Ende
- Zeichenfolgen auf der Tastatur

Achten sollte man

- Verschiedenes Passwort für verschiedene Systeme!
- ändern Sie regelmäßig das Passwort

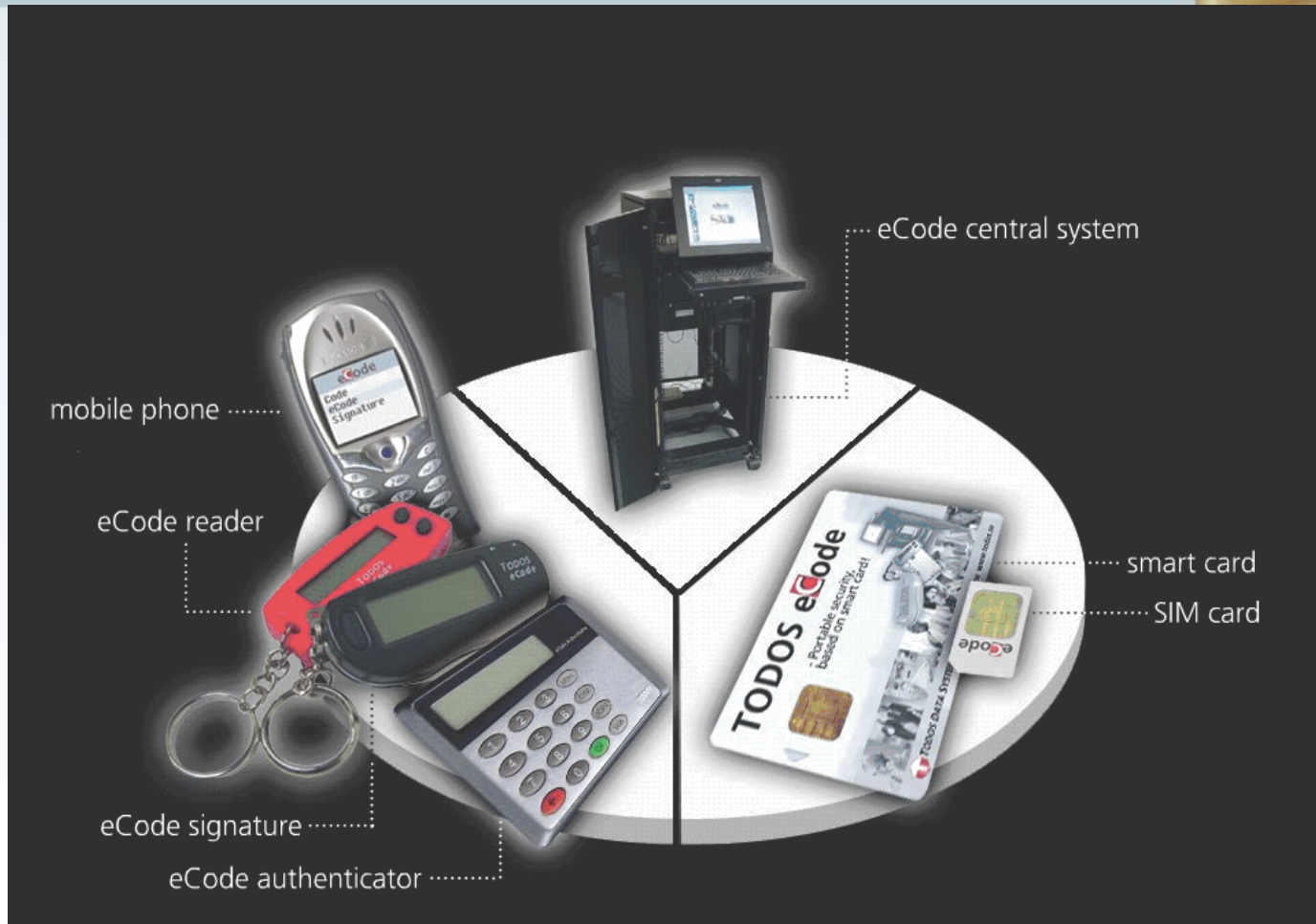
Anforderungen an ein Passwort (2)



ein paar Tricks

- Das Ersetzen von Buchstaben durch Sonderzeichen:
LIEBE = L!EBE
- Das Einfügen von Zahlen in der Mitte:
Boz99TOL
- Das Ersetzen von „phonetische“ Lauten:
Achtung! = 8tung!
- Die Kombination mehrere Tricks:
dieser Sommer `99 ist sehr heiß = d\$`99ish

One Time Code - System

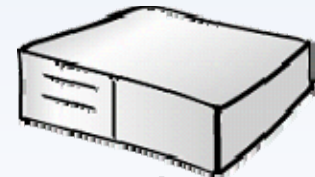


2. eCode wird beim Einstieg ins Online Banking 1 x verwendet

3. User und eCode wird an Bankserver weitergeleitet



Online Banking Server



4. Bankserver überprüft Korrektheit des eCodes bei eCode Server



eCode Server

IT Security Day - Folie 46

1. Chipkarte wird in Lesegerät eingeführt PIN eingegeben und eCode wird angezeigt



Das OTC-System



12233456

12485456

34264267

89658578

45678569

50389756

03276072

98756251

06709083

65231659

67156459

78256234

09523657

66759432

56473256

97423657

84325420

39856237

85612965

79816234

12514623

46435463

