



# Covert Channels in elektronischen Ausweisen

Klaus Schmeh, cv cryptovision

17. DFN Workshop „Sicherheit in vernetzen Systemen“

Hamburg 09./10.02.2010

Herr Müller erfüllte die Anforderungen  
stets zu vollsten Zufriedenheit.



Hans Maier, Geschäftsführer

Herr Müller erfüllte die Anforderungen  
stets zu vollsten Zufriedenheit.

A handwritten signature in blue ink that reads "Hans Maier". The signature is written in a cursive style with a large initial 'H'.

Hans Maier, Geschäftsführer

# Covert Channel

Kommunikationsmittel in einer Umgebung, in der Kommunikation ...

- nicht vorgesehen ist
- verboten ist
- technisch verhindert wird

# Covert Channel

Ähnliche Begriffe:

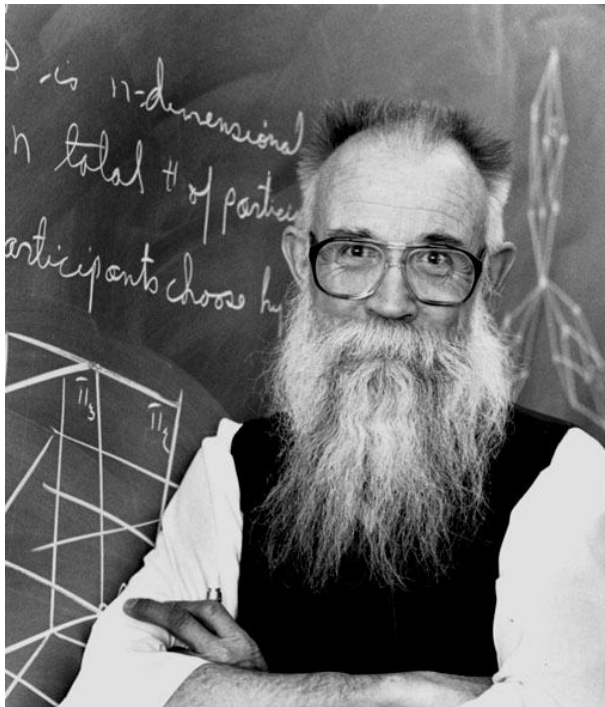
- Subliminal Channel
- Steganografie
- parasitärer Kommunikationskanal

# Covert Channels



**Butler Lampson**  
führte 1973 den Begriff Covert Channel ein

## Covert Channels



**Gus Simmons**  
erforschte Covert Channels

# Elektronische Ausweise

Ausweis



Chip





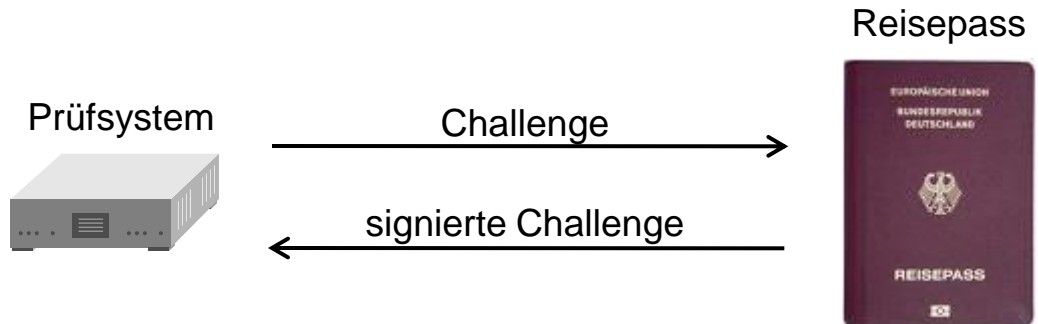
Gibt es Covert Channels im Zusammenhang mit elektronischen Ausweisen?



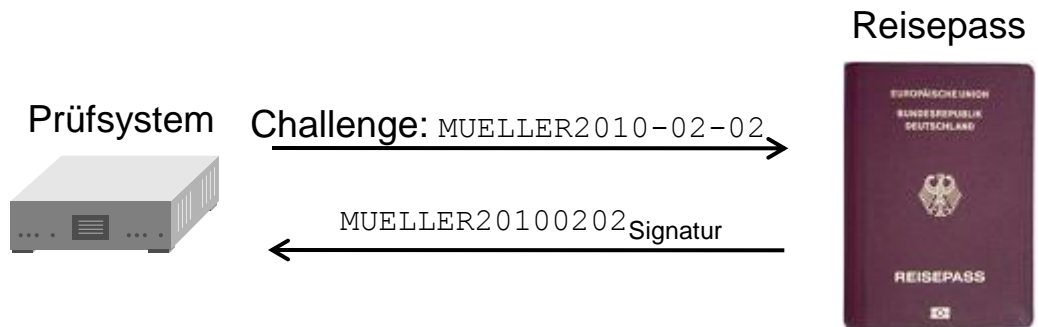
Chip in der  
Passdecke

Symbol für  
elektronisches  
Passbuch

# Active Authentication



# Active Authentication



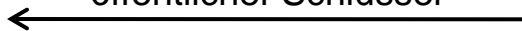
# Chip Authentication



öffentlicher Schlüssel



öffentlicher Schlüssel





# Elektronische Gesundheitskarte

Möglichkeiten für Covert Channels:

- elektronisches Rezept
- elektronisches Patientenfach
- elektronischer Arztbrief
- ...





# E-Ausweise in Europa



Belgium (BELPIC)



Spain (DNIe)



Finland (FINEID)



Estonia (ESTEID)



Portugal (Cartão de cidadão)

# Digitale Signatur

	RSA	DSA	ECDSA
Covert Channel	+	++	++

# DSA-Signatur

A5 D6 03 0B C5 D6 23 0B A8 D6 3A 5D 63 31 B3 0B A8 D6 3A 5D



10 Bit



# Optische Speicherstreifen



?

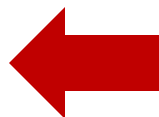


# Covert Channel in einem Foto

01001100 11110101 11010101  
10011100 11100100 101001010  
10001101 11110100 110101010  
10011001 11101001 111101100  
11001101 11110100 110101010  
10011001 11101001 110101010  
11001100 11110100 110101010  
00011010 11110100 110101010  
11001100 11010101 110101010  
01011001 11110100 110101010  
11001010 11110100 111101000  
01001100 11110100 110101010  
01001101 11110100 110101010

01001101 11110100 110101011  
10011100 11100100 101001010  
10001101 11110100 110101010  
10011001 11101001 111101100  
11001101 11110100 110101010  
10011001 11101001 110101010  
11001101 11110100 110101011  
00011010 11110100 110101010  
11001100 11010101 110101010  
01011001 11110100 110101010  
11001010 11110100 111101000  
01001100 11110100 110101010  
01001100 11110101 110101011

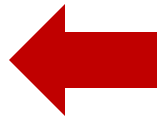
# Foto



# Covert Channel im Passfoto



# Nutzung eines Covert Channel für digitale Wasserzeichen

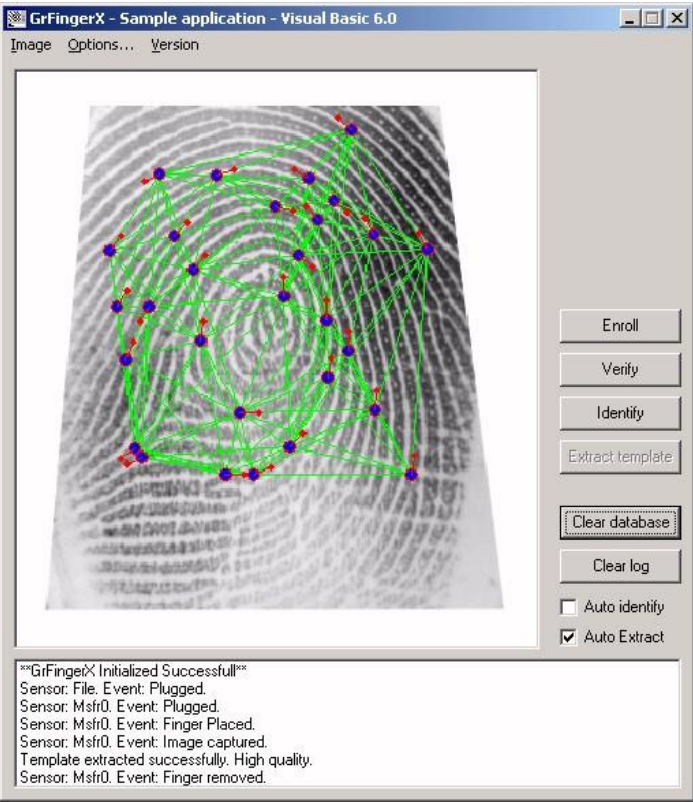




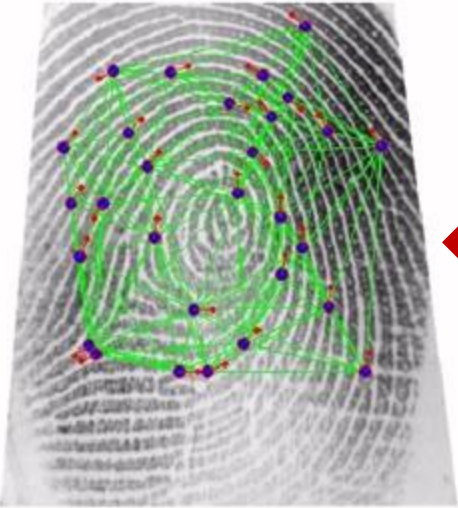




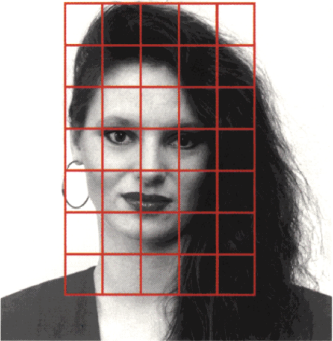
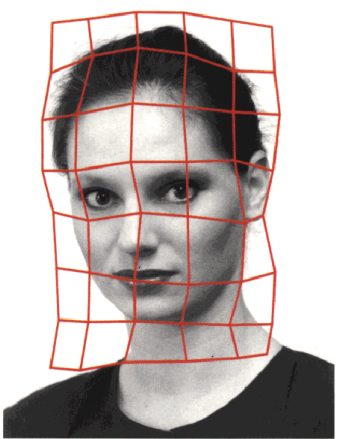
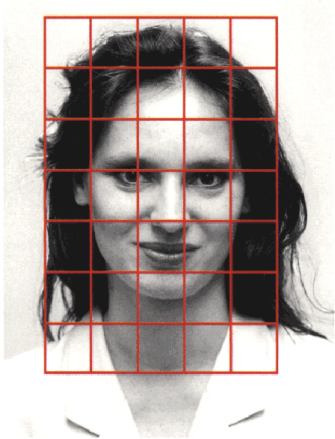
# Biometrische Templates



# Biometrische Templates



# Biometrische Templates







## Weitere Möglichkeiten



- Magnetstreifen
- unsichtbare Markierungen
- Position und Größe von Buchstaben minimal variieren

# Paul Müller



## Fazit



- Covert Channels auf e-IDs in vielfältiger Weise möglich
- Nutzung für Wasserzeichen hat sich nicht durchgesetzt
- Gefahren sind vorhanden, jedoch meist tolerierbar
- Transparenz ist das beste Gegenmittel





