

# Potenzial des Kontaktlos-Chip

Univ.-Doz. D.I. Dr. **Ernst Piller**

Vorsitzender des österr. Chipkartenverbandes (ASA)

Institutsvorstand an der Fachhochschule St. Pölten

Geschäftsführer der Smart-ID, [www.smart-id.at](http://www.smart-id.at)

Michael-Bernhard-Gasse 10, 1120 Wien

Matthias Corvinus-Strasse 15, 3100 St. Pölten

Tel.: 0664 9200891



# Warum Chipkarten?

- Aus dem großen Bedarf nach einer sicheren Identifikation, die eine sichere Authentifizierung erfordert → Chipkarten wie SIM-Karten, Bankkarten, Unternehmenskarten, Schüler/Studentenkarten usw.
- Chipkarte erlaubt mehrstufige Authentifikation (z.B.: PIN oder Biometrie vom Benutzer und Challenge & Response zum IT System)

# Warum Chipkarten?

- Aus dem großen Bedarf nach hochsicherer Rechenleistung vor Ort auf einem Kleinstcomputer für die Erzeugung einer Digitalen Signatur, für elektronische Geldbörsen (z.B.: Quick), zur Überprüfung von biometrischen Daten, für die Datenverschlüsselung, für die kryptografische Identifikation/Authentifizierung,

.....

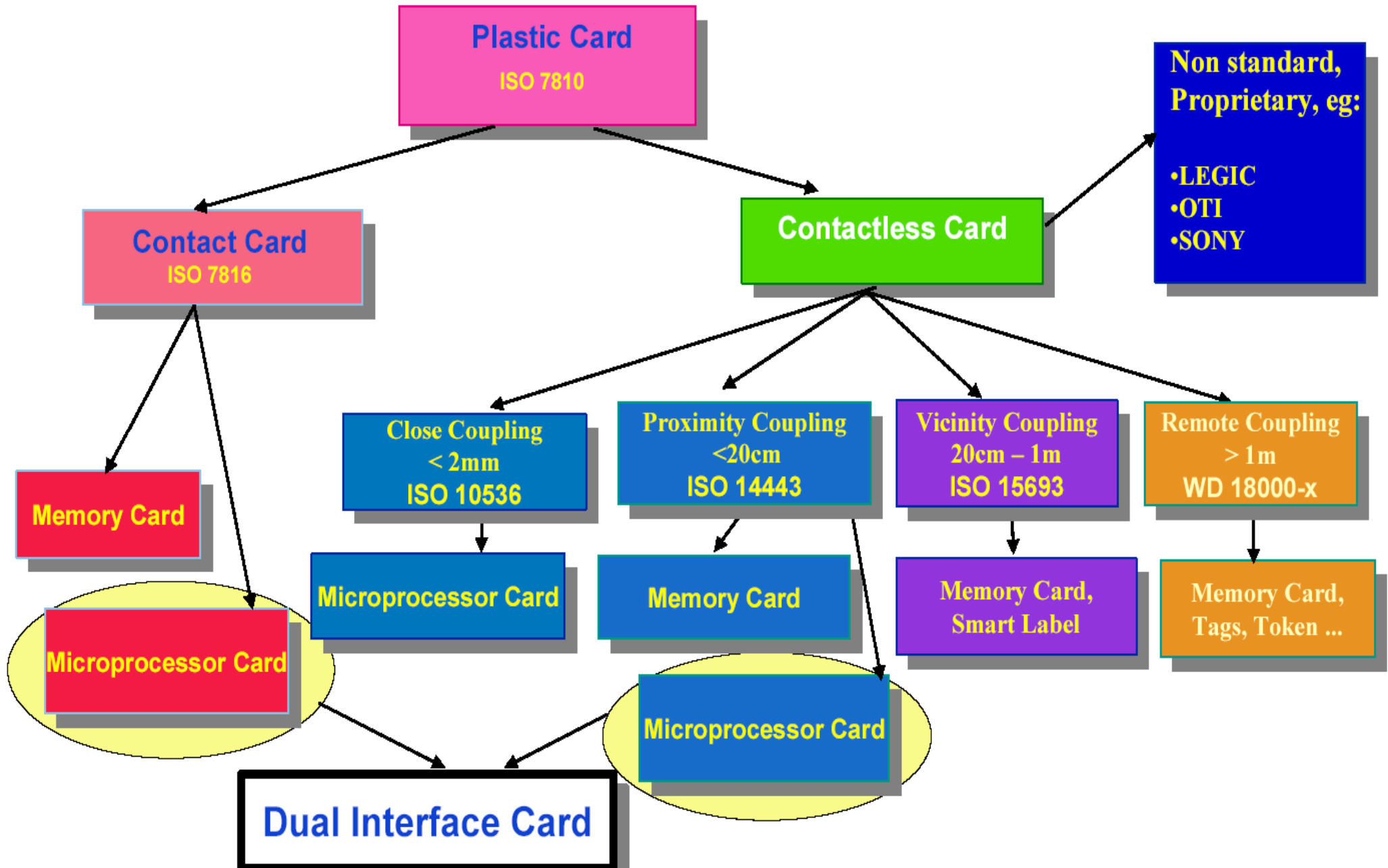
# Warum Chipkarten?

- Aus dem Bedarf nach geschützten Daten vor Ort wie kryptografische Daten, PINs / Passwörter, Karteninhaberdaten, Zertifikate, Zahlungsverkehrsdaten (Limite, Beträge, Kontodaten etc.), Berechtigten, Tickets, medizinische Daten, Benutzerprofile, Protokolle, sonstige Daten
- Daraus ergibt sich auch die Möglichkeit einer Benutzer-Anonymisierung

# Chipkarte - der persönliche Sicherheitstoken in der digitalen Welt

- Chipkarte ist ideales Medium zur informationellen Selbstbestimmung, d.h. nur in Verbindung mit der Chipkarte können Daten lokal und global gelesen und weiter verarbeitet werden und dies bei Bedarf auch auf anonyme Weise
- Eine „total“ digitalisierte und vernetzte Welt ist ohne umfangreichen Schutz völlig offen für Betrug, Spionage, Sabotage, ... → IT Sicherheit ist extrem wichtiges Thema und **Chipkarte kann dabei wichtige Beiträge leisten**

# Übersicht Chipkarten



# Klassische kontaktbehaftete Chipkarten

- SIM-Karte, USIM-Karte für mobile Telekomm.
- Bankkarte: Kreditkarte, Debitkarte, Geldbörse, ...
- Versicherungskarte (e-card)
- Mitarbeiterkarte (Kantine, PC-Benutzung, IT-Anwendungen, PKI-Anwendungen, ....)
- Studentenkarte, Schülerkarte
- Pay-TV Card
- Sonstige Karten: Tourismuskarten, Nofallkarten, Clubkarten, ...



**ASA**

Austrian Smart-Card Association



Verein zur Förderung von Chipkarteninnovationen

# Klassische Kontaktlos-Chipkarten

- Reisepass mit Chip (und sonstige Ausweise in Zukunft wie Führerschein, Personalausweis)
- Mitarbeiterkarte
- Schülerkarte, Studentenkarte
- Tourismuskarte (z.B. Ski-Ticket), Eventkarte, Ausweis für öffentliche Einrichtungen (z.B. Schwimmbad) etc.
- .....



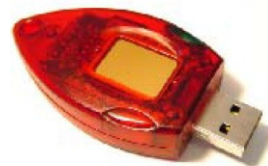
# Hauptanwendungen Kontaktlos-Chipkarten

- Physikalische Zutrittsberechtigung:  
Parkplätze, Gebäude, Räume, Tresore etc.
- Berechtigung (+ Abrechnung): Auto,  
Maschinen, Kopierer, Telefon, Lift, PCs,  
Laboreinrichtungen, Entlehnung (Bibliothek,  
Geräte), .....
- Öffentlicher Nahverkehr: Ticket, Zeitkarte, ...
- RFID für Dinge: Logistik, Inventur, Verleih,  
Diebstahlschutz, Standortlokalisierung,  
Instandhaltung, .....



# RFID und neue Chipkartenformate

- SIM-Karte war erste Abweichung von Ur-Größe
- Chipkarte auch in anderen Größen heute erfolgreich mit einem enormen Wachstum z.B. Reisepass, USB-Gerät, Autoschlüssel, Uhr, Band, RFID-Ticket, ....
- „Chipkarte“ für Tiere
- „Chipkarte“ für Dinge wie RFID-Tag, Nagel, Scheibe, ...



# NFC (Near Field Communication)

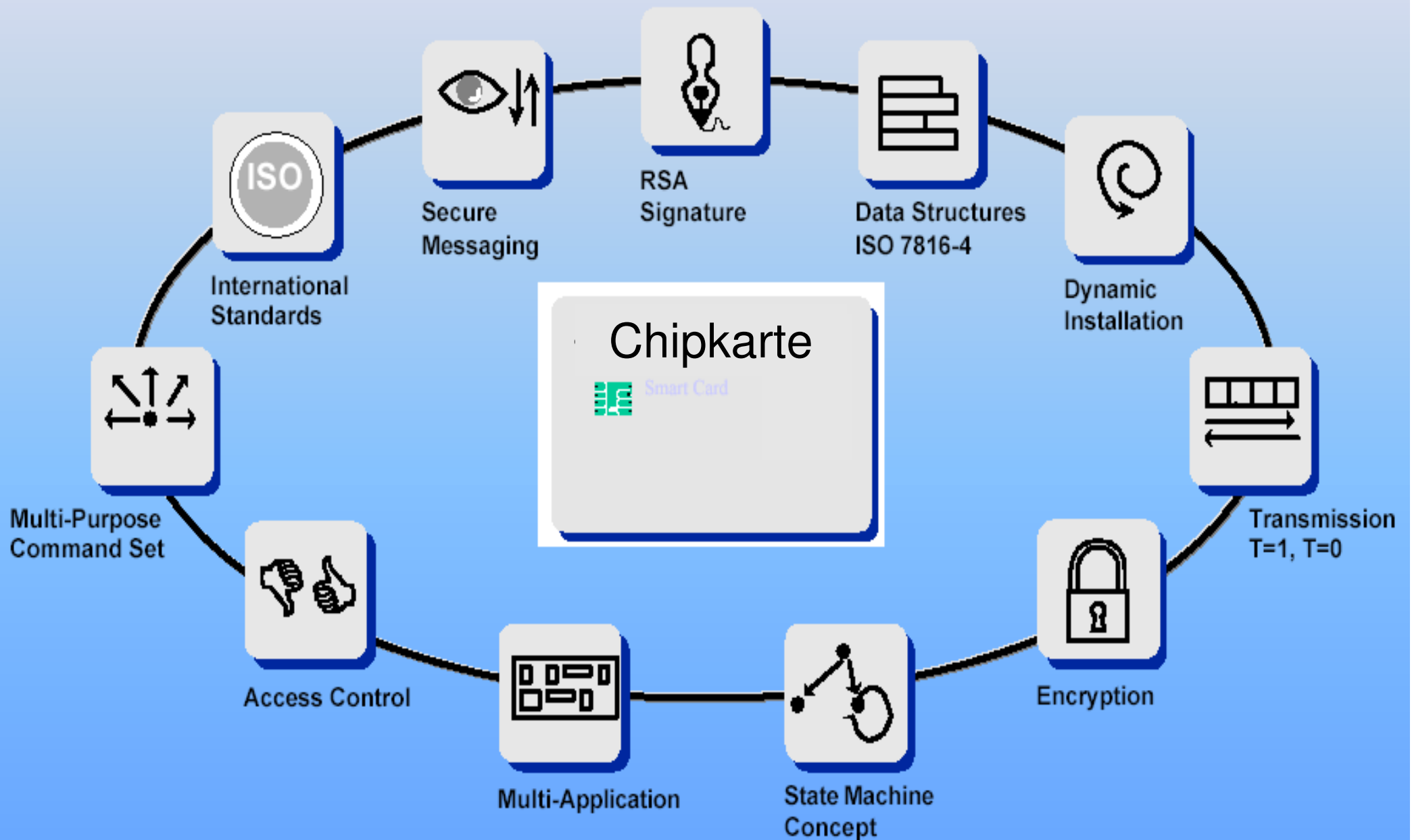
- Direkte Kommunikation zwischen Laptop, Handy, PDA, Media-Center (TV, Video, ...), etc.
- Direkte Kommunikation dieser Geräte mit Kontaktlos-Chipkarten
- **NFC-Handy wird zur Chipkarte**



# Sicherheit von Chipkarten

- Von Chipkarten erwartet man hohe Sicherheit
- Klassische Chipkarten-Anwendungen wie Ausweis, Zahlungsverkehr, Mobil-Telefonie, Zutrittskontrolle erfordern höchste Sicherheit
- Da rund 5 Milliarden Chipkarten in derartigen Anwendungen im Einsatz sind, kann bei erfolgreichem Angriff ein großer Schaden entstehen
- Muster für Angriffsversuche über Internet erhältlich

# Sicherheitsmechanismen



# Kontaktlos-Chipkarten: Angriffe und Gegenmaßnahmen

<b>Angriffsmöglichkeiten</b>	<b>Gegenmaßnahmen</b>
Abhören der Kommunikation und Analyse der Daten	Verschlüsselung, geringe Entfernung
Unautorisierte Kommunikation (z.B. Zahlvorgang)	Dynamische gegenseitige kryptografische Authentifikation, Willenserklärung (PIN, Biometrie, Bewegung, Taste etc.)
Diebstahl Karte	Passwort, Online, Sperrlisten
Cloning und Emulation	Dyn. kryptogr. Authentifikation
Manipulation der Kommunikation	MAC, Digitale Signatur
Zeit-/Stromanalysen, .....	HW-Mechanismen
Zerstörung durch Feldeinwirkung	Selbstheilende Sicherung

# Vorstellung der ASA: Österreichischer Chipkartenverband

- Gründung: 1984
- Veranstalter von bisher 23 Chipkartentagungen
- Veranstalter von Seminaren und Kursen über Chipkarten und Lösungen
- Lobbying, Beratung von Mitgliedern, .....
- Jährliche Vergabe eines Chipkarten-Preises
- Homepage: [www.asa.or.at](http://www.asa.or.at)



**Ich danke Ihnen für das Interesse  
und für Ihre Aufmerksamkeit**