XTC-ID Handbuch

Leitfaden zur RFID-System Integration

Dieses Werk entstand im Rahmen des Projektes XTC-ID (eXtended Temperature Chip IDentification), welches von 2017 bis 2021 über das INTERREG V Programm der EUREGIO grenzüberschreitend gefördert wurde. Das Handbuch soll den interessierten Lesern zunächst einen Überblick zum aktuellen Stand der RFID-Technologie aufzeigen und anschließend die innovative XTC-ID-Technologie anhand von praxistauglichen Applikationen vorstellen. Neben detaillierten Beschreibungen zu einer möglichen System Integration in industriellen Anwendungen, wurde im ersten Kapitel „RFID für Dummies“ besonderen Wert auf eine leicht verständliche Einführung für den interessierten „Einsteiger“ gelegt. Unser Anliegen ist es dabei, dem Leser das volle Potential von RFID, gerade auch für den Einsatz im privaten Umfeld, zu erschließen.

Dr. Martin Paplewski (Intelli Labs Deutschland) im Dezember 2020

XTC-ID
Xtreme
RFID

Europäische Union
Europese Unie

WWW.DEUTSCHLAND-NEDERLAND.EU

Dieses Projekt wird im Rahmen des INTERREG-Programms von der Europäischen Union und den INTERREG-Partnern finanziell unterstützt.

Dit project wordt in het kader van het INTERREG-programma financieel ondersteund door de Europese Unie en de INTERREG-partners.

Version 1.8 – Oktober 2021

Die Projektpartner:

IMST
Institut für Mobil- & Satelliten Funk Technik
Prof. Dr. Ingo Wolff

dnl contact
Dr. Johannes Reef

Intelli Labs
Dr. Martin Paplewski

jsb
Joint Analytical Systems Benelux
Ing. Marco Koenen

University of Twente
Enschede - The Netherlands
Prof. Dr. Jurriaan Schmitz

Mit Unterstützung durch:

INTERREG Deutschland Nederland

Europäische Union
Europese Unie

Ministerium für Wirtschaft, Energie, Industrie, Mittelstand und Handwerk des Landes Nordrhein-Westfalen

Ministerie van Economische Zaken

PROVINCIE FLEVOLAND

Provincie Noord-Brabant

Inhaltsverzeichnis

1. RFID für „Dummies“

1.1 Historische Entwicklung

Obwohl die sogenannte RFID (Radio Frequency Identification) Technologie schon seit Anfang der 90er Jahre in immer mehr Bereiche des öffentlichen Lebens vordringt, herrscht bis heute oftmals Unkenntnis bezüglich des Potentials, aber auch der Risiken bei ihren Einsatz. Dies hat zunächst historische Ursachen, da wie jede neue Technologie so auch die RFID, erst mehrere Evolutionsstufen durchlaufen musste, bis eine stetige Marktdurchdringung erfolgte. So war bis ca. 2008 die Entwicklung neuer Anwendungen für spezifische Märkte vornehmlich den Fachexperten vorbehalten, die aufgrund fehlender Standarisierung oftmals auf proprietäre Lösungen setzten. Beispiele für solche Anwendungen finden sich noch heute in Form elektronischer Wegfahrsperren im KFZ-Bereich, oder bei der Kodierung von Haus- und Nutztieren. Ein gewöhnlicher Benutzer kam wenn überhaupt, mit RFID nur in Form von fertigen „Black Box“ Lösungen in Kontakt, ohne sich um die zugrunde liegende Technik überhaupt Gedanken machen zu müssen. Da aber die steigende Zahl an proprietären Lösungen zunehmend die Erschließung weiterer Märkte z.B. durch Kompatibilitäts-probleme blockierte, wurde die Entwicklung eines Standards immer dringender.

Dies gelang um die Jahrtausendwende, erstmals für die damals neue Hoch-Frequenz (HF) Technik, in Form mehrerer ISO-Standarisierungen. Letztendlich begann der Siegeszug der HF-RFID-Chips wie wir sie heute kennen, aber erst im Jahr 2008 mit Veröffentlichung des sogenannten NFC-Standards, durch ein Konsortium der Unternehmen NXP (vormals Phillips) und Sony. Basierend auf den älteren ISO-Standards, die vornehmlich technische & elektronische Spezifikationen beschreiben, beinhaltet NFC (Near Field Communication oder Nah Feld Kommunikation) nun auch ein standarisiertes, einfach zu implementierendes Datenprotokoll. Schon zum Zeitpunkt der Veröffentlichung war damit klar, dass NFC vor allem für den Einsatz im „Consumer“-Markt, beispielweise für die gerade erst erschienenen Smartphones, konzipiert wurde. Trotzdem dauerte es noch fünf Jahre, bis am 27. April 2013 erstmals ein Android Smartphone mit integrierter NFC-Funktionalität (Samsung Galaxy S4) vorgestellt wurde. Eigentlich, so hätte man vermuten können, stand ab diesem Zeitpunkt nichts mehr einem flächendeckenden Einsatz in Massenmärkten entgegen. Anders als gedacht, führt die NFC-Technologie aber bis heute, eher ein Schattendasein. Zum einen fehlt die Akzeptanz in Teilen der Bevölkerung aufgrund von Datenschutz Bedenken oder Verletzung von Persönlichkeitsrechten bei vielen Digitalisierungsvorhaben, zum anderen und das ist unseres Erachtens die häufigste Ursache, herrscht allgemeine Unkenntnis darüber, wie NFC überhaupt funktioniert und welches Potential im täglichen Einsatz damit erschlossen werden könnte. Diese Technologie steht nämlich nicht nur Behörden (elektronischer Personalausweis) oder großen Organisationen (kontaktloses Bezahlen) offen, vielmehr lassen sich auch private Anwendungen beispielweise im smart-Home Bereich, damit einfach und kostengünstig von jedermann generieren. Wie so etwas funktioniert und welche Komponenten benötigt werden, erfährt der geschätzte Leser in den nächsten Unterkapiteln, anhand von Praxisbeispielen aus dem Alltag des Autors.

1.2 Funktion und Technik

Um eine komplexe Technologie als „Laie“ richtig einschätzen zu können, gilt es diese wenigstens rudimentär zu erfassen und zunächst von verwirrenden fachspezifischen, zudem meist fremdsprachlichen Abkürzungen zu entschlacken. Hilfreich ist es oftmals mit einer Übersetzung des Oberbegriffes zu beginnen, in unserem Fall also RFID „Radio Frequenz Identifikation“. Umgangssprachlich übersetzt ergibt sich daraus eine „Identifikation mittels Radiofrequenzen“ bzw. Radiowellen. Anders ausgedrückt wird im einfachsten Fall ein Objekt mittels Funkwellen drahtlos erkannt. In Analogie zum Radio dreht man solange am Frequenzregler, bis sich die Inhalte einer Sendestation empfangen lassen. Während beim Radioempfang einzelne Sender in einem breiten Frequenzband verteilt sind, existieren im Fall der RFID nur drei spezifische Frequenzen (siehe Kapitel 2). Diese drei Frequenzen definieren zudem den Typ der RFID-Technologie. Ein Abgleich zwischen Sender und Empfänger wie beim Radio, ist werksseitig schon berücksichtigt und nicht mehr notwendig. Andererseits lassen sich dadurch Bauteile und Geräte für eine Frequenz, nicht mit denen anderer mischen. Für unsere Heimanwendungen beschränken wir uns deshalb auf die HF-Frequenz bei 13.56 MHz, mit der auch die NFC-Technik arbeitet.

Die nächste Frage, die sich in Analogie zum Radio nun unweigerlich stellt, gilt dem Auffinden des Senders und Empfängers. Also den beiden Teilen, die man zwingend für ein funktionierendes RFID-System benötigt. Auf den ersten Blick gestaltet sich die Suche etwas schwierig. Eigentlich erwartet man, dass zum Betrieb elektronischer Komponenten auf beiden Seiten eine Spannungsversorgung vorhanden sein muss. Während beim Smartphone als typisches Lesegerät (fachlich „Reader“) der Fall klar ist, sucht man auf der Gegenseite, wie beispielsweise den EC-Karten (Abb. 1) vergeblich nach einer Stromquelle. Diese Eigenschaft stellt ein herausragendes Merkmal passiver RFID-Transponder den sogenannten TAG’s dar. Sie befinden sich am zu identifizierenden Objekt und besitzen keine eigene Stromversorgung oder Batterie! Vielmehr wird erst beim Zugriff auf den TAG, der zum Betrieb notwendige Strom aus den abgestrahlten Funkwellen (Erregerfeld) des Readers erzeugt. Es handelt sich hierbei um das gleiche Prinzip, wie es aktuell zum kabellosen Laden (QI-Laden) von Smartphones verwendet wird. Ohne Erregerfeld ist also z.B. ein NFC-TAG nichts mehr als ein „*toter*“ Gegenstand, der erst bei Annäherung an einen Reader „*zum Leben*“ erweckt wird.

Abb. 1) Röntgenbild einer EC-Karte mit HF-RFID TAG

Wie aus der Abb. 1 deutlich zu erkennen ist, sind solche TAG's sehr einfach aufgebaut. Sie bestehen prinzipiell nur aus einer elektrisch leitfähigen Antennenstruktur, die im einfachsten Fall auch aus einer kleinen Drahtspule mit typischerweise sechs Wicklungen bestehen kann sowie einem daran angebrachten Silizium-Chip. Ein solcher Chip besitzt immer eine weltweit eindeutige Seriennummer, die ab Werk bereits fest „eingebrannt" wurde und nicht veränderbar ist. Ähnlich wie bei Netzwerkkarten in Form der MAC-Adresse, lassen sich anhand dieses 64 Bit (8 Bytes) langen UID-Kodes (aufgebaut aus 16 hexadezimale Zeichen A-F & 0-9) gekennzeichnete Objekte eindeutig identifizieren. Zusätzlich sind insbesondere die NFC-TAG's, häufig mit einem wiederbeschreibbaren Datenspeicher mit Speicherinhalten ab 180 Bytes versehen. Damit sind schon in der Grundversion Datensätze von 180 reinen Textzeichen möglich. Dieser Speicher lässt sich zudem mit einem NFC-fähigen Smartphone sowie der passenden App selbst auslesen, beschreiben, schützen oder löschen. Wie später noch vorgestellt wird, lassen sich außer reinen Datensätzen aber auch Steuerfunktionen zum Auslösen bestimmter Ereignisse im Speicher ablegen. Diese Möglichkeit erlaubt die eigenständige Entwicklung vieler interessanter Applikationen rund um das Thema smart-Home und IoT (Internet der Dinge).

Einfach erklärt, lässt sich ein RFID-TAG auch mit einem kleinen, kabellosen und zugleich wiederverwendbaren USB-Stick vergleichen, auf dem sich beliebige Daten ablegen und wieder auslesen lassen. Diese Merkmale sowie die Möglichkeit TAG's auch versteckt anbringen und durch nicht metallische Materialien hindurch auf diese zugreifen zu können, sind wesentliche Unterschiede zu den ebenfalls sehr gebräuchlichen QR-Barcodes. Zu beachten ist, dass bei aktivierter RFID-Funktion im Smartphone oder Reader, eine automatische Kommunikation direkt erfolgt, sobald ein TAG in Reichweite ist! Im Gegensatz zu Barcodes, bei dem ein Anwender selbstständig unter direktem Sichtkontakt scannen muss, ist in diesem Fall keine weitere Interaktion nötig. Dieses Verhalten ist eine grundlegende technische Eigenschaft aller bekannten RFID-Typen und ermöglicht erst die einfache Erfassung von markierten Objekten durch eine selbstständige „Kontaktaufnahme". Gerade für Applikationen im privaten oder vertraulichen Umfeld ist ein solches Verhalten aber unerwünscht oder gar gefährlich (Datenschutz & Privatsphäre). Es stellt deshalb mit den Hauptgrund für die ablehnende Haltung einiger Bevölkerungsgruppen zum Einsatz der RFID-Technologie dar und ist ein steter Quell von Mythen und Halbwahrheiten (Kapitel 1.3).

Um dieser Problematik zu begegnen wurde letztendlich der NFC-Standard entwickelt. Die Abkürzung steht wörtlich übersetzt für Nahbereichs Kommunikation und bedeutet im Wesentlichen nichts anderes, als das TAG und Reader erst unter einem Abstand von typischerweise kleiner 15 mm miteinander kommunizieren können. Im Idealfall, beispielsweise mit größeren Antennen und höherer Sendeleistung, sind unter bestmöglichen Bedingungen teilweise auch Reichweiten von einigen Zentimetern möglich. Trotzdem muss ein Anwender immer erst ein Objekt mit dem NFC-TAG (z.B. die Kreditkarte) nahe genug an ein Lesegerät bringen, um die Kommunikation zu ermöglichen. Dadurch, dass der Benutzer erst selbst aktiv werden muss, ist ein ungewollter oder illegaler Zugriff praktisch ausgeschlossen. Dieser zusätzliche Sicherheitsaspekt wird also durch eine geringe Reichweite erkauft, ermöglicht andererseits aber erst die Digitalisierung von Dienstleistungen im privaten Umfeld. Aus diesem Grund finden im öffentlichen Alltag heutzutage ausschließlich NFC-TAG's Verwendung, die im Fall von sicherheitsrelevanten Anwendungen zudem noch kryptologische

Sicherheitsfunktionen im Chip integriert haben. Zu dieser Klasse gehören unter anderem der elektronische Personalausweis oder Reisepass, EC- und Kreditkarten sowie alle neuen Ausweise der Krankenkassen. Obwohl auch hier alle Anwendungen dem standarisierten NFC-Protokoll folgen, kann ohne entsprechenden Schlüssel nicht auf die gespeicherten Datensätze zugegriffen werden. Da die technischen Chipspezifikationen wie Hersteller, Typ, Speichergröße, Sicherheitsfunktionen usw. immer unverschlüsselt im „Header" zugänglich sein müssen, kann jedermann aber leicht mittels Smartphone selbst überprüfen, ob ein NFC-TAG vorhanden ist oder nicht (Abb. 2).

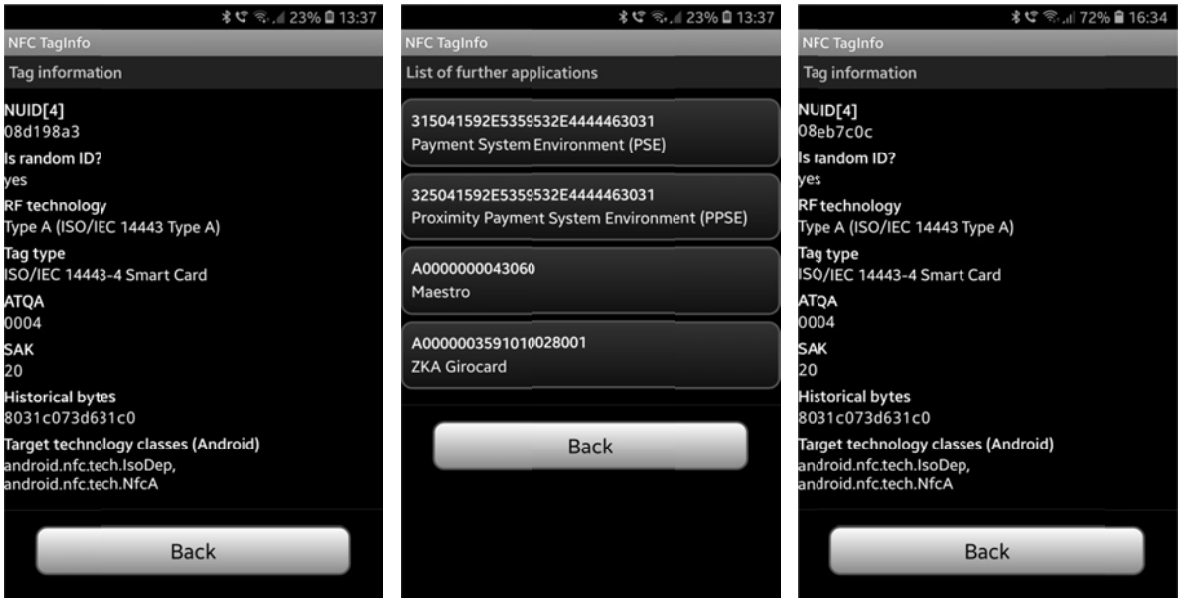


Abb. 2) ausgelesene NFC Chip-Daten der EC-Karte aus Abb. 1 im zeitlichen Abstand

Betrachtet man sich die TAG Informationen aus Abbildung 2 fällt als Besonderheit auf, dass die ID-Nummer nach ISO 14443-A nur 4 Bytes lang ist. Eine solche NUID (Non-Unique Identifier) Seriennummer wäre mit den maximal 3,7 Milliarden möglichen Kombinationen nicht unbedingt einzigartig. Um die Sicherheit bei kritischen Applikationen zu erhöhen, wird deshalb bei jedem Zugriff oder genauer bei jedem Reader-Feldwechsel, eine neue zufällige ID generiert (Random ID). Wie im rechten Bild zu sehen, ergibt das erneute Auslesen mit dem Smartphone bei Zeitstempel 16:34 Uhr auch richtigerweise eine andere NUID. Das UID0 Byte = 0x08 bleibt dabei immer identisch und charakterisiert die Random ID Funktionalität des Chips.

Es bleibt nun noch die eingangs gestellte Frage nach Sender und Empfänger zu klären. Im RFID-Kontext können beide Gegenstellen, also „Reader" und Transponder (TAG) immer beides sein. Obwohl beim Ausdruck „Reader" eigentlich ein reines Lesegerät erwartet wird, hat dieser hardwareseitig **immer** eine Lese- und Schreibfunktionalität. Es ist hier natürlich dem Hersteller überlassen, diese Funktionalität softwaretechnisch einzuschränken, wie es beispielsweise Apple im Fall der iPhones über das iOS Betriebssystem praktiziert. Mit einem NFC-fähigen Smartphone ist es also möglich einen TAG nicht nur zu lesen sondern auch zu beschreiben, soweit es die Sicherheitskonfiguration zulässt. Bei unbenutzten NFC-TAG's lassen sich selbst diese Einstellungen mittels App konfigurieren. Auf der Gegenseite dem Transponder abgekürzt TAG, ergibt sich die duale Eigenschaft schon aus den zusammengesetzten englischen Begriffen „Transmit" (Senden) und

„Respond“ (Reagieren). Ein TAG reagiert auf das elektromagnetische Feld eines Readers zunächst durch Erzeugung einer Versorgungsspannung, dem Empfang von Kommandos und dem Senden der ID Nummer und eventuell gespeicherter Dateninhalte. Als Erweiterung des NFC-Protokolls kann ein TAG aber auch auf einen Reader reagieren (Ereignis) und dann direkt mit diesem durch programmierte Steuerbefehle agieren (Aktion).

1.3 Mythen und Fakten

Im gleichen Maße wie die RFID-Technologie, insbesondere durch Einführung der kontaktlosen Bezahlsysteme, immer mehr das private Umfeld durchdringt, nimmt auch die Intensität der Diskussion in den sozialen Medien weiter an Fahrt auf. Dabei werden vornehmlich negative Effekte, wie Datendiebstahl oder Eingriffe in die Privatsphäre thematisiert und teils aus Unkenntnis heraus mit haarsträubenden Argumenten begründet. Infolge der Komplexität der RFID-Technologie lassen sich dabei auch nicht einzelne Aussagen, eins zu eins auf alle Arten von RFID Anwendungen übertragen. Glücklicherweise kommen Privatpersonen, insbesondere durch die weite Verbreitung mobiler Endgeräte und deren Apps, heute fast ausnahmslos nur noch mit NFC Standard kompatiblen HF-Transpondern (TAG) in Kontakt, während andere Frequenzbereiche bislang ausschließlich industriellen oder logistischen Applikationen vorbehalten sind. Da zudem die unterschiedlichen RFID-Technologien zueinander inkompatibel sind, d.h. ein NFC-TAG lässt sich z.B. nicht mit einem UHF-fähigen Lesegerät auslesen und umgekehrt, wird an dieser Stelle ausschließlich die Nahfeld-kommunikation (NFC) betrachtet. Der Vollständigkeit halber soll allerdings nicht unerwähnt bleiben, dass die Massenapplikation der schlüssellosen (key-less) Wegfahrsperren, selbst in modernen Fahrzeugen, noch immer auf eine zwar proprietäre, aber technologisch doch veraltete „low-frequency“ (LF) Technologie aufsetzt. Wie einige Untersuchungsberichte zeigen, lassen sich solche Systeme mit einem noch vertretbaren technischen Aufwand überbrücken, so dass weitere Sicherheitssysteme in den Fahrzeugen notwendig wurden, um einen ausreichenden Diebstahlschutz zu erreichen. Um die Akzeptanz der Bevölkerung gegenüber der RFID-Technologie weiter zu erhöhen, wäre es empfehlenswert, bei allen sicherheitskritischen oder Datenschutz rechtlichen relevanten Applikationen direkt auf die, im vorherigen Kapitel vorgestellten, RFID-Chips mit kryptographischer Funktionalität zu setzen.

Obwohl die verwendeten NFC-TAGs in aktuellen Kreditkarten, Ausweisdokumenten und ähnlichen einen solch hohen Sicherheitsstandard erfüllen, finden sich im Zubehörhandel eine Vielzahl an Artikeln, angefangen von Schutzhüllen bis hin zu ferromagnetischen Folien, die mit einem wirksamen Schutz gegen „Datenklau“ oder Datenmissbrauch beworben werden. Es stellt sich somit die Frage, ob ein solcher zusätzlicher Schutz tatsächlich notwendig ist, oder es sich hier nur um eine gut angesetzte Marketingstrategie handelt. Auch hier lässt sich am besten wieder die alte Binsenwahrheit, „Probieren geht über Studieren“ zu Rate ziehen. Glücklicherweise kann jeder Besitzer eines NFC-fähigen Smartphones sich selbst einmal in die Lage eines Datendiebes versetzten und versuchen, seine Kreditkarte durch die Geldbörse hindurch auszulesen. Ein Erfolg dürfte in diesem Fall recht zweifelhaft sein, insbesondere wenn zusätzlich noch Münzen oder weitere NFC bestückte Karten darin aufbewahrt werden. Ebenso dürfte der Einsatz speziell aufgerüsteter Technik, z.B. in Form von größeren Antennen und leistungsstärkeren Lesegeräten überschaubar bleiben, da die vielleicht unter

günstigsten Umständen gewonnenen Daten wertlos sind (Abb. 2) und keine persönlichen Informationen enthalten. Für einen Datendiebstahl steht hier der notwendige Aufwand in keiner Relation zum Gewinn. Viel erfolgsversprechender wäre es in diesem Fall, entweder die Kreditkarte gleich zu stehlen, oder die Kommunikation des Kartenlesegerätes mit dem Backbone Netzwerk des Zahlungsdienstleisters zu manipulieren. Hier hilft dann aber auch keine Schutzhülle.

Anders als gedacht und beworben, machen abschirmende Schutzhüllen dagegen Sinn, wenn es darum geht den eigentlichen NFC-TAG gegen starke elektromagnetische Felder zu schützen. Es steht also nicht der Schutz gegen Datendiebstahl sondern gegen Fremdeinwirkung im Vordergrund, um beispielsweise die Funktion einer Kreditkarte zu erhalten. Solche elektromagnetischen Felder können nicht nur an speziellen Industriearbeitsplätzen vorliegen, sondern auch in Krankenhäuser und Arztpraxen z.B. in der Nähe von Kernspintomographen oder Röntgengeräten auftreten. Auch haushaltsübliche Mikrowellengeräte sind geeignet, einen NFC-TAG ohne sichtbare Beschädigung in Sekundenbruchteilen zu zerstören. Obwohl Mikrowellengeräte typischerweise bei einer Hauptfrequenz von 2.4 GHz arbeiten, reicht die innerhalb der Antenne induzierte Energie bei weitem aus, um die nach ISO/IEC 14443 oder 15693 maximale elektromagnetische Feldstärke von 12 A/m bei 13.56 MHz, deutlich zu überschreiten. Schon nach ca. drei Sekunden in einer 900 Watt Mikrowelle wird die Verlustwärme am Eingangswiderstand des Chips so groß, dass der Transponder thermisch zerstört wird. So benutzen Personen, die aus Datenschutzgründen die digitale Ausweisfunktion beim elektronischen Personalausweis ablehnen dieses einfache Verfahren um den Chip zu deaktivieren, aber gleichzeitig die analoge Funktionalität zu erhalten. Ein Nachweis ob ein solcher Defekt dann absichtlich oder unabsichtlich z.B. infolge äußerer Einflüsse erfolgte, ist natürlich nicht mehr möglich. Mit Hilfe der im folgenden Kapitel vorgestellten Methoden kann aber jeder leicht selber nachprüfen, ob überhaupt ein NFC-TAG vorhanden ist und wenn ja, dieser noch funktioniert.

Wichtig ist es letztendlich, wie übrigens bei jeder anderen Technologie auch, die Akzeptanz des Anwenders zu gewinnen. Dies gelingt grundsätzlich umso besser, je mehr direkte Vorteile sich bei jedem einzelnen durch ihre Verwendung ergeben. Eventuell gegenüberstehende Nachteile sollten aber klar benannt werden, um jeden Interessenten in die Lage zu versetzen, auch selbstständig eine Nutzen- / Risikoabschätzung durchzuführen und somit einen verantwortungsvollen Gebrauch der Technologie zu ermöglichen. Diesem Ziel hat sich das nachfolgende Kapitel „smarte NFC-Applikationen für den Privatanwender“ verschrieben. Die dort aufgeführten Beispiele sind sozusagen als Nebenprodukte, während der Laufzeit des XTC-ID Projektes angefallen und sollen das Potential der NFC-Basistechnologie, gerade auch für den Einsatz im alltäglichen Umfeld aufzeigen. Der Kreativität des Lesers sind dabei keine Grenzen gesetzt, denn die technologischen Hürden sowie der Preisfaktor zur Umsetzung innovativer Ideen sind gering.

Ein weiteres positives Detail sollte in diesem Zusammenhang nicht unerwähnt bleiben. Trotz häufig gegenteiliger Nachrichten bezüglich unseres Nachholbedarfs bei den digitalen Technologien sowie der elektronischen Bauteilfertigung, ist Europa auf dem Gebiet der RFID immer noch führend. Neben den beiden größten Chipherstellern Infineon (München, DE) und NPS (Eindhoven, NL), stammt der Großteil an qualitativ hochwertigen Smartphone NFC-Apps ebenfalls aus Europa. Lassen Sie uns gemeinsam diesen Vorsprung auch in Zukunft weiter ausbauen.

1.4 smarte NFC-Applikationen für den Privatanwender

1.4.1 Detektion von NFC-TAGs mit dem Smartphone

Seitdem Google im Jahr 2010 erstmals standardmäßig einen NFC-Reader Chip in den Modellen ihrer Nexus Serie verbaute, finden sich diese nun seit 2014 fast ausnahmslos in jedem modernen Smartphone wieder. Ob z.B. ein Android Smartphone den NFC-Standard unterstützt, lässt sich dabei leicht in den System Einstellungen überprüfen. Unter dem Menüpunkt <**Verbindungen**> sollte sich in diesem Fall ein Eintrag „**NFC und Zahlung**“ finden lassen, unter dem sich die NFC-Funktionalität aktivieren lässt. Meistens reicht aber schon ein Blick in die Schnelleinstellungen beim herunterscrollen der oberen Statuszeile (die mit dem Batteriesymbol), um das standarisierte NFC Icon ℕ nach Abbildung 3 zu finden und ebenso das Protokoll ein- oder auszuschalten.

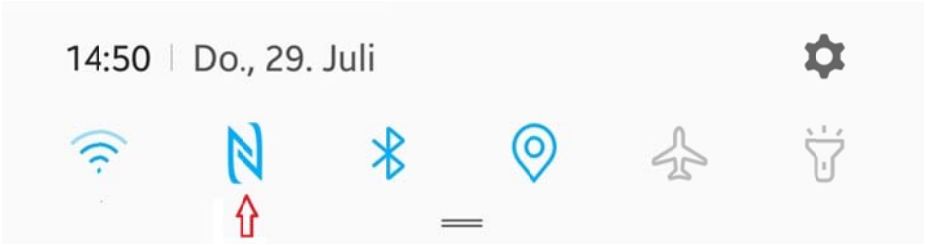


Abb. 3) aktiviertes NFC-Protokoll in den Android Schnelleinstellungen

Etwas schwieriger gestaltet sich die Situation dagegen bei **Apple iPhones**. Im Gegensatz zu Android hat Apple bei ihrem iOS den NFC-Standard über einen langen Zeitraum hinweg nicht unterstützt bzw. freigegeben. Das ist umso überraschender, da alle iPhones spätestens ab dem iPhone 6, werksmäßig ebenfalls mit NFC-Hardware ausgerüstet wurden. Mit **iOS 13** wurde letztendlich die NFC-Unterstützung ausgebaut und kann, neben dem favorisierten kontaktlosen Bezahlen mittels Apple Pay, nun auch eingeschränkt für eigene Zwecke genutzt werden. So lassen sich jetzt auch NFC-Tags **ab dem iPhone 7** auslesen oder beschreiben. Für die alten iPhones 6 und 6s gibt es dagegen keine Möglichkeit zum Beschreiben von NFC-Tags. Die NFC-Funktion ist dabei standardmäßig aktiviert und lässt sich, anders als bei Android hier nicht ausschalten! Daraus wird deutlich, dass Apple noch immer die Apple Pay Funktion als Hauptanwendungsgebiet der NFC-Technologie versteht. Demzufolge beschränkt sich auch die Anzahl an verfügbaren NFC-Apps im Jahr 2020 bislang auf gerade einmal zehn Einträge im App Store. Quantität ist aber nicht alles. Auch im App Store gibt es einige qualitative hochwertige Apps, die für den Privatgebrauch geeignet sind und zusammen mit den Android Versionen im weiteren Verlauf vorgestellt werden. Für stolze Besitzer eines aktuellen Gerätes, ist zudem überhaupt keine NFC-App mehr notwendig um z.B. einen TAG auszulesen. Analog zu den Android Geräten, werden auch hier die gespeicherten Informationen direkt aus dem TAG abgerufen und entweder in einem Meldungsfenster angezeigt, oder gleich an eine dafür vorgesehene App weitergereicht. Hierzu gehören das iPhone XS (Max), iPhone XR, iPhone 11 (Pro und Pro Max) und iPhone SE 2. Ebenso wurde ab iOS 13 die integrierte Kurzbefehle-App für diese Geräte, um Befehle zur NFC-Automatisation erweitert. Soviel zunächst zu den technischen Voraussetzungen der Smartphones. Falls noch nicht erfolgt, aktivieren wir jetzt die NFC-Verbindung am Smartphone und stöbern einmal in der Brieftasche nach Ausweisen und Karten mit „versteckten“ NFC-TAGs. Um die Erfolgschancen bei ersten Versuchen zu erhöhen, empfiehlt sich zunächst die Auswahl einer

Kreditkarte mit aufgedrucktem kontaktlos Symbol , bei der mit Sicherheit ein NFC-TAG verbaut sein sollte. Alternativ kann man natürlich auch direkt den, der Druckauflage im Einband beigelegten, NFC-Aufkleber benutzen. Anschließend geht es darum die ungefähre Position der NFC-Antenne im Smartphone zu ermitteln. Diese unterscheiden sich leider je nach Modell deutlich voneinander, so dass einige Leseversuche notwendig sein können. Infolge der geringen Reichweite sowie auftretenden Abschirmeffekten vom Smartphone Gehäuse, sollten ebenfalls eventuell vorhandene Schutzhüllen von der Rückseite des Gerätes entfernt werden. Zudem beschränken viele Hersteller die Feldstärke der NFC-Chips, um die Akkulaufzeit positiv zu beeinflussen. Das führt leider dazu, dass insbesondere die Kommunikation mit dem Online-Personalausweis (eID) instabil wird oder gar nicht funktioniert. Empfehlenswert ist es deshalb, eingeschaltete Energiesparmodi zunächst zu deaktivieren, um ein Gefühl für Reichweite und Erkennungsrate zu gewinnen. In Samsung Geräten ist die NFC-Antenne zusammen mit der QI-Ladefunktion meistens mittig auf der Rückseite verbaut, während bei Apple iPhones und chinesischen Herstellern wie Huawei oder Xiaomi, sich diese zum Beispiel nahe der rückwärtigen Kameralinse am oberen Rand befinden (Abb. 4). Bei älteren Geräten wie dem Samsung Galaxy S4, kann die Antenne auch mit im auswechselbaren Akku integriert sein.

Abb. 4) typische NFC-Antennenpositionen bei Smartphones

Typischerweise legt man das zu lesende Objekt zunächst mittig auf die **Rückseite** des Smartphones an. Da selbst bei aktiviertem NFC, das Betriebssystem nicht ständig auf einen NFC-TAG im Erregerfeld prüft, kommt es zu einer kurzzeitlichen Verzögerung von ca. 2 Sekunden, bis eine Erkennung stattfindet. Es ist hier wichtig die Position für einige Sekunden zu halten bis der Lesevorgang komplett abgeschlossen wurde. Abhängig von den Smartphone Einstellungen, erfolgt dann direkt eine Benachrichtigung mittels Signalton und/oder Vibrationsalarm sowie die Ausgabe der eingelesenen Nachricht in einem Pop-Up Fenster. Wird dabei keine passende App zur Nachrichtenausgabe gefunden, wird stattdessen die Fehlermeldung *„Keine unterstützte App für diesen NFC-Tag“* angezeigt. In diesem Fall empfiehlt sich die Installation einer der nachfolgend vorgestellten Basis-Apps aus dem Play- oder App-Store.

Abb. 5) App-Auswahl Fenster nach Erkennung

Sind dagegen mehrere Apps gleicher Funktionalität installiert, so wird standardmäßig ein Auswahlfenster "*Aktion durchführen mit...*" zur Weiterverarbeitung angezeigt (Abb. 5). In diesem Fall lässt

sich optional auch gleich die Standardaktion für diesen Nachrichtentyp festlegen, wodurch beim nächsten Scanvorgang direkt die dort eingestellte App geöffnet wird. Unabhängig vom verwendeten Smartphone, erzielen von den fünf verfügbaren NFC Forum TAG Typen, die aktuellen Typ 5 TAG Varianten nach SO/IEC 15693 (Vicinity Standard) die höchsten Reichweiten und sollten gegebenenfalls für eigene Anwendungen bevorzugt werden.

Als Basis-App für Android Smartphones, bietet sich zunächst die werbefreie und frei verfügbare App, „**NFC TagInfo“** vom österreichischen Entwickler Michael Roland an. Obwohl letztmals 2014 aktualisiert, zeichnet sich diese durch eine hohe Kompatibilität und Erkennungsrate für unterschiedlichste RFID-TAGs aus. So werden nicht nur NFC Forum Typen, sondern auch viele proprietäre ISO/IEC HF TAGs erkannt und ihre technischen Spezifikationen ausgelesen. Die App kann kostenlos im Google Play Store heruntergeladen werden (Abb. 6), steht für iPhones aber leider nicht zur Verfügung.

Abb. 6) NFC TagInfo für Android – Download Link
https://play.google.com/store/apps/details?id=com.nxp.taginfolite

Die App „NFC TagInfo“ lässt sich einfach bedienen und ermöglicht bei kompatiblen und unverschlüsselten TAGs, die Anzeige der ausgelesenen Rohdaten in verschiedenen Formaten (ASCII, HEX, UTF-8) sowie die blockweise Auflistung der Speicherinhalte (Abb. 7). Weiterhin sind detaillierte Informationen über den TAG Typ, der Speichergröße sowie zum Status der eventuell aktivierter Sonderfunktionen wie z.B. dem Schreib-/Leseschutz ersichtlich. Da die App nur eine reine Lesefunktionalität bietet, ist zudem eine Beschädigung der NFC-Daten ausgeschlossen. Sie eignet sich somit in idealer Weise als leistungsfähiger **TAG Detektor** für allgemeine Anwendungen.

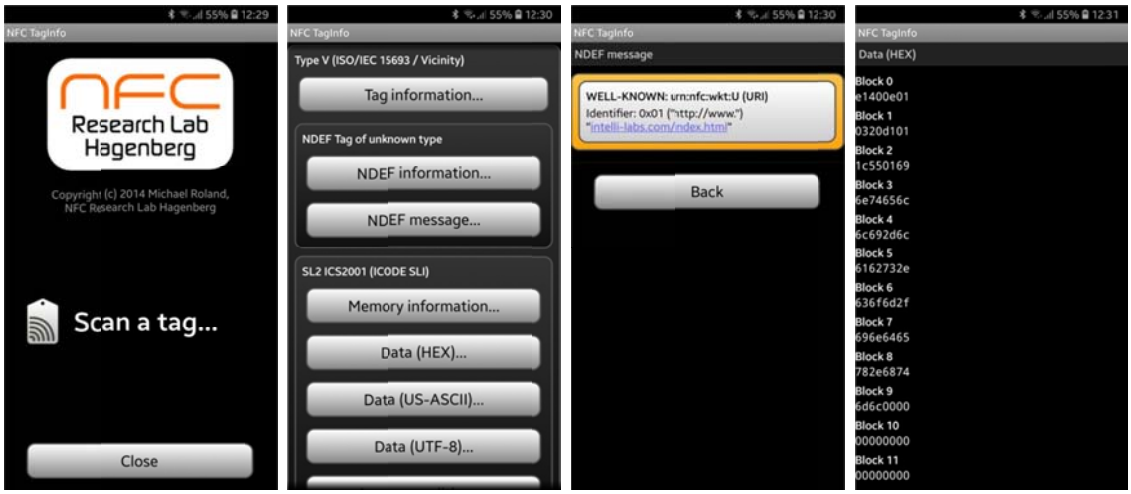


Abb. 7) NFC TagInfo für Android – Funktionsumfang

Als weitere erstklassige Basis-App **unter Android und iOS**, ist die fast gleichnamige Applikation „**NFC TAGInfo**“ von NXP (Eindhoven, NL), einem der weltweit größten TAG Hersteller, zu nennen. Im Gegensatz zur vorher beschriebenen App, wird diese regelmäßig aktualisiert und unterstützt dadurch auch alle neuen NFC-Forum Typen 4 und 5. Die App kann ebenfalls kostenlos aus dem Google Play Store oder dem Apple App Store heruntergeladen werden (Abb. 8).

Abb. 8) NFC TagInfo by NXP für Android und iOS – Download Links
https://play.google.com/store/apps/details?id=com.nxp.taginfolite
https://apps.apple.com/de/app/nfc-taginfo-by-nxp/id1246143596

Auch in dieser App werden alle wichtigen TAG Informationen sowie alle Speicherblöcke mit Lesezugriff in verschiedenen Formaten ausgegeben. Die kompletten Daten können zudem als Datensatz lokal auf dem Smartphone abgespeichert werden (Abb. 9/Screen EXTRA aus Historie) Etwas gewöhnungsbedürftig ist hier allerdings, dass die wichtige TAG-ID Nummer nicht unter dem Menüpunkt <IC INFO>, sondern erst im <FULL SCAN> Menü auftaucht. Obwohl diese während der Kommunikation grundsätzlich immer als erstes geprüft wird und so die eindeutige Identifizierung des TAGs für spätere Zugriffe sicherstellt. Doch dieser Schönheitsfehler stellt die Qualität der App in keiner Weise in Frage. Gerade aufgrund der detailliert aufgeschlüsselten Informationen, die sonst nur mit hohem Aufwand ermittelt werden können, ist die App nicht nur für Entwickler interessant, sondern auch für den normalen Anwender bei der Fehlersuche empfehlenswert!

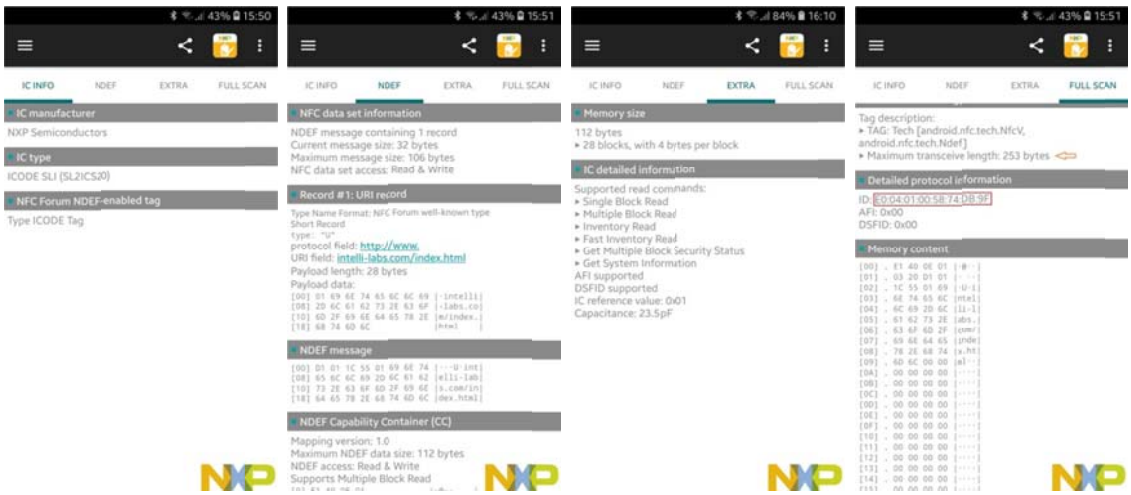


Abb. 9) NFC TagInfo by NXP (Android Version)

1.4.2 e-ID Personalausweis

Seit Oktober 2010 wird in Deutschland der Personalausweis nur noch mit integriertem RFID-TAG ausgegeben. Neben persönlichen und biometrischen Daten (hoheitliche Funktionen), wurde auch direkt eine Online-Ausweisfunktion integriert, die vom Inhaber des Ausweises aber erst optional angefordert werden musste. Nach Beendigung der Einführungsphase, sind seit 2017 alle neu ausgegebenen Ausweise automatisch für die sogenannte Online-ID oder auch eID (nicht-hoheitliche Funktion) freigeschaltet. Eine 6-stellige PIN zur erstmaligen Aktivierung wird dem Inhaber separat per Post zugestellt. Im Unterschied dazu hat der elektronische Reisepass zwar ebenfalls einen integrierten RFID-TAG zur Speicherung biometrischer Daten, er ist aber nicht Online-ID fähig.

Durch den Elektronischen Identitätsnachweis (eID-Funktion) soll sich Bürgern eine sichere Möglichkeit bieten, sich im Internet gegenüber Behörden, Online-Shops oder Online-Dienstanbietern eindeutig zu authentifizieren. Folgende Applikationen werden damit abgedeckt:

- **Identitätsnachweis**: Bürger können mit ihrem neuen Personalausweis Ihre Identität auch im Internet eindeutig nachweisen und können beispielsweise online ein Bankkonto eröffnen.
- **Altersverifikation**: Über die eID-Funktion kann einem Internetanbieter ein eventuell erforderlicher Altersnachweis des Kunden übermittelt werden.
- **Formularfunktion**: Mit der eID im Personalausweis, können Anträge an das Bürger- oder Finanzamt online gestellt und gleichzeitig direkt authentifiziert werden.
- **Login**: Alternativ zu den bekannten Benutzernamen und Passwörtern können Nutzer auch einfach die eID-Funktion nutzen, um sich im Internet einzuloggen. Ebenfalls möglich ist es, sich bei verschiedenen Dienstanbietern unter einem Pseudonym einzuloggen und so einen hohen Datenschutz Faktor zu erzielen. Für jeden Dienstanbieter generiert der Personalausweis dabei automatisch ein eigenes Pseudonym!

Der elektronische Identitätsnachweis basiert auf einer gegenseitigen Authentifizierung, sodass sowohl Anbieter als auch Nutzer abgesichert sind. Im **ersten Schritt** ermittelt dabei das Bundesverwaltungsamt die Echtheit eines Anbieters und stellt diesem sodann ein Berechtigungszertifikat aus. Erst dieses Zertifikat berechtigt einen Anbieter überhaupt Daten von einem Nutzer anzufragen. Nach Nutzer Interaktion wird diesem im **zweiten Schritt** das Berechtigungszertifikat übermittelt. Daraufhin platziert der Nutzer seinen Personalausweis auf ein Lesegerät und die AusweisApp2 liest die erforderlichen Daten vom RFID-Chip des Ausweises. Dem Nutzer wird angezeigt, welche Daten an den Anbieter übermittelt werden. Erst nach anschließender PIN-Eingabe wird durch die AusweisApp2 eine sichere Verbindung zu einem eID-Server aufgebaut und die Daten verschlüsselt übermittelt. In diesem Fall wird für den gesicherten Kommunikationskanal das Sicherheitsprotokoll Passwort Authenticated Connection Establishment (PACE) verwendet.

Zur Nutzung der Online-ID Funktion ist immer eine spezielle **AusweisApp2** erforderlich, die unter dem Link *https://www.ausweisapp.bund.de/ausweisapp2/* erhältlich ist. Neben weiteren Informationen findet sich dort unter anderem auch deren Open-Source Code. Da diese App aufgrund ihrer hohen Datenverschlüsselungstechnologie besondere Hard- und Softwareanforderungen benötigt, empfiehlt sich vor deren Installation eine Prüfung der Smartphone Kompatibilität mit der

gerade vorgestellten „NFC TagInfo by NXP“ App. Im Personalausweis befindet sich der RFID-TAG im oberen rechten Bereich unterhalb der Ausweisnummer (Abb. 10).

Abb. 10) Personalausweis mit gekennzeichneter Chip Platzierung

Das Ergebnis des Scans eines Personalausweises aus Q4/2020 ist in Abb. 11 dargestellt. Je nach Ausstellungsdatum sind in den Personalausweisen unterschiedliche Chip-Typen verbaut, entweder vom Hersteller NXP Semiconductors (NXP P60D145) oder Infineon Technologies (IFX SLC52). Aufgrund sicherheitstechnischer Vorgaben ist mit „normalen“ Apps kein Zugriff auf verschlüsselte Speicherbereiche möglich und nur allgemeine technische Informationen auslesbar. Diese reichen aber aus, um die Kompatibilität des Smartphones mit dem Online-ID Verfahren zu überprüfen.

Abb. 11) Personalausweis Scan mit NFC TagInfo by NXP (Android Version)

Wurde der Ausweis dabei fehlerfrei gelesen, ist die Antennen Feldstärke des Smartphones ausreichend, um den erhöhten Energiebedarf dieser RFID-Chips abzudecken. Weiterhin entscheidend ist der Byte-Wert für die „**Extended length**„ Kommunikation. Dieser muss mindestens 500 Byte betragen, um das PACE Verschlüsselungsprotokoll auszuführen. Im Menü <FULL SCAN> unter „*Android technology information*“ finden sich die entsprechenden Einträge (Abb. 11). Mit 65279 Bytes „Maximum transceive length“ sowie der „Extended length APDU“ Unterstützung ist selbst das hier verwendete, ältere Samsung Galaxy S7 Online-ID fähig. Sollte dagegen der Erfolg ausbleiben, hilft eventuell noch ein Android Firmware Update (ab Android 9) oder nur ein neueres Smartphone.

1.4.3 Beschreiben von NFC-TAGs mit dem Smartphone

Das Beschreiben von NFC-TAGs mit eigenen Daten, in Form sogenannter **NDEF Nachrichten**, gestaltet sich mit der richtigen App genauso einfach, wie das Auslesen derselben. Zwingend erforderlich ist neben einem NFC-fähigen Smartphone, natürlich ein ungesperrter (löschbarer) oder neuer TAG. Je nach Speichergröße, sind diese ab ca. einem Euro bei verschiedenen Online Händler, auch in geringen Stückzahlen erhältlich. Da der Preisunterschied eines größeren Chip-Speichers prinzipiell vernachlässigbar ist, empfiehlt sich gerade am Anfang die Investition in Typen mit 924 Bytes oder höherer Kapazität. Abzüglich des Speicherverbrauchs der Blockverwaltung nach NDEF-Formatierung, bleiben hiervon 868 Bytes zur freien Verfügung nutzbar. Das entspricht einer Kapazität von 868 ASCII Zeichen (UTF-8 Bit) und damit in etwa der Länge dieses Absatzes bis hier. Die Anzahl scheint im ersten Augenblick überschaubar zu sein, sie reicht aber dennoch für die meisten Anwendungen aus, zumal dieser Wert nur eine grobe Abschätzung liefert. Ebenso lässt sich auch mit proprietärer Software, bei Verzicht auf die NDEF-Formatierung, die gesamte Speicherkapazität nutzen.

Besitzer eines aktuellen iPhones (ab XS, XR, SE, 11 Pro & Pro Max) mit iOS 13 können an dieser Stelle direkt loslegen, ohne vorher eine entsprechende App zu installieren. Die Funktion ist in der systemeigenen Kurzbefehle-App unter <Automation> zu finden. Dabei können folgende Aktionen direkt programmiert werden:

- Internet Links öffnen
- Kontaktdaten schreiben (Visitenkarte)
- Verbindung zu WLAN-Netzwerke herstellen
- SMS verschicken*
- Telefonnummer anrufen
- eigenen Text anzeigen
- Geo-Daten (Ort/Position) ablegen

*Infolge geänderter Google Nutzungsbedingungen, ist der automatische SMS-Versand per NFC Ereignis für Android Apps aus dem Play Store schon nicht mehr zulässig. Inwieweit Apple hier ebenfalls Einschränkungen plant, konnte bislang nicht evaluiert werden.

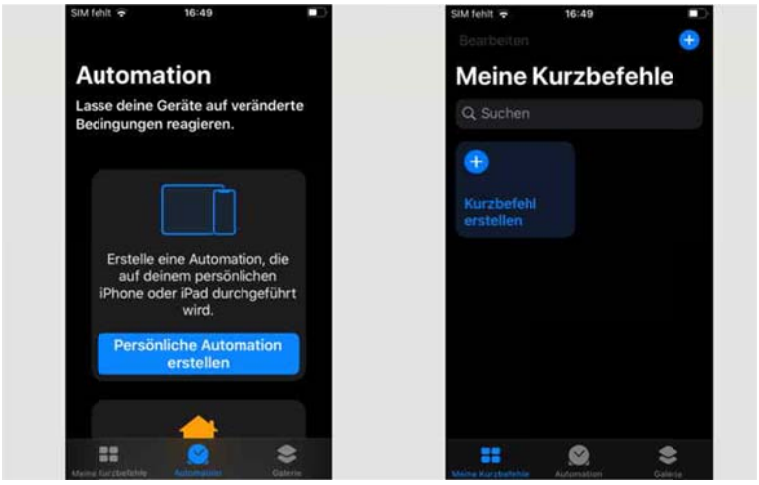


Abb. 12) Automation Startseite in der Kurzbefehle-App (iOS 13 Version)

Zur Erstellung eines eigenen Kurzbefehls sind nachstehende Schritte durchzuführen, wobei sich von Schritt 5 bis 7 der TAG permanent im Antennenfeld befinden muss:

1) In der Kurzbefehl-App den Eintrag Automationen aufrufen
2) Hier eine Persönliche Automation erstellen (Abb. 12)
3) NFC auswählen
4) Schaltfläche <Scannen> betätigen
5) NFC-TAG an das iPhone anlegen, Antennenposition beachten (Abb. 4)
6) einen Namen für den TAG vergeben
7) eine auszuführende Aktion hinzufügen

Für alle iPhones bei denen die NFC Automation in der Kurzbefehl-App nicht unterstützt wird, oder für Benutzer, die eine erweiterte Funktionalität benötigen, empfiehlt sich ein Blick in den App Store unter „**NFC für iPhone**“. Diese bietet ab iPhone 7 einen erweiterten Befehlsumfang und deutlich mehr Konfigurationsmöglichkeiten.

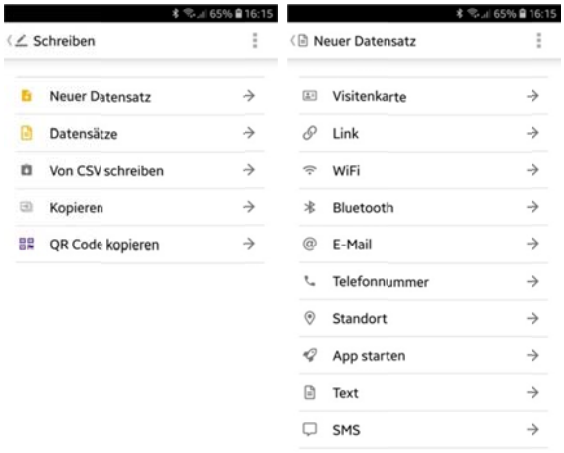
Abb. 13) NFC für iPhone – Download Link App Store
https://apps.apple.com/de/app/nfc-für-iphone/id1249686798

Doch auch zum Beschreiben von NFC-TAGs, gibt es vom Chiphersteller NXP die kostenlose „**NFC-TagWriter**“ App sowohl für Android als auch iOS, in regelmäßig aktualisierten Versionen (Abb. 14). Neben dem Schreiben standarisierter NDEF-Nachrichten für eine Vielzahl unterschiedlicher Aktionen, sind auch spezielle Verwaltungsfunktionen (Schreib- und Passwortschutz, Sperrung blockieren usw.) für NXP kompatible Chips vorhanden. **Wichtig für alle bislang vorgestellten Apps ist allerdings die Einschränkung, dass nur eine Aktion pro Scan ausgeführt werden kann**! Infolge von Limitationen im NDEF-Format, ist bei diesem Standard eine komplette smart-HOME Automatisierung, beispielsweise die Ausführung als Befehlsfolge, nicht möglich. Für Android gibt es in diesem Kontext jedoch hervorragende Alternativen, mit allerdings proprietären Formaten. Der interessierte Leser sei hierzu auf das smart-CAR Kapitel verwiesen.

Abb. 14) NFC TagWriter by NXP für Android und iOS – Download Links
https://play.google.com/store/apps/details?id=com.nxp.nfc.tagwriter
https://apps.apple.com/de/app/nfc-tagwriter-by-nxp/id1246143221

1.4.4 Applikationen im NDEF-Format

Unter Verwendung der „**NFC-TagWriter**“ App werden an dieser Stelle nun zwar einfache, aber oft auch recht nützliche Anwendungen im sogenannten NDEF-Format vorgestellt. Wie im letzten Kapitel erwähnt, hat dieses Format zwar die Limitation, dass sich jeweils nur eine Aktion bzw. Nachricht pro Scan ausführen lässt, dafür laufen aber alle vorhandenen Aktionstypen auf jedem NFC kompatiblen Smartphone und zwar ohne vorherige Installation zusätzlicher Apps. Anders ausgedrückt wird zum Beschreiben des TAGs zwar meistens eine spezielle App benötigt, dagegen aber nicht beim Lesen, beispielsweise mit einem fremden Smartphone. Die möglichen programmierbaren Aktionen beschränken sich hier also auf grundlegende, schon im Betriebssystem vorinstallierte Systemfunktionen. Eine Übersicht dieser Funktionen kann der Abbildung 15 entnommen werden.



Kontaktdaten aus Telefonbuch übertragen
Internetlink (z.B. Webseite) im Browser öffnen
WLAN Verbindung automatisch herstellen
Bluetooth Kopplung automatisch durchführen
vorgefertigte E-Mail versenden
abgelegte Telefonnummer anrufen
abgelegte Ortskoordinaten in Karten-App aufrufen
eine beliebige installierte App ausführen
gespeicherte Textnotiz anzeigen
SMS Kurznachricht senden

Abb. 15) NDEF-Standard Aktionsliste (Android Version)

Im ersten Versuch werden wir nun umgehend unsere Visitenkarte mit einer smarten Funktion „aufpimpen“. Dazu eigenen sich besonders NFC-Aufkleber, die beispielsweise auf der Rückseite einer herkömmlichen Visitenkarte geklebt werden können. Je nach Ausführung ist die Oberseite des Aufklebers auch bedruckbar, so dass dort ebenfalls noch ein Logo oder Barcode Platz findet. Nach unseren Testerfahrungen funktionieren neben Tintenstrahl- auch Laserdrucker zum Beschriften. Zwingend notwendig ist dagegen die Verwendung eines Einzelblatteinzuges, um Beschädigungen des TAGs zu verhindern. Nach dem Starten der App, wird der so vorbereitete TAG anschließend unter der Menüauswahl <Schreiben> <Neuer Datensatz> <Visitenkarte> mit einem ausgewählten Kontaktdatensatz aus dem Telefonbuch beschrieben (Abb. 16). Eine vorherige Formatierung unter Löschung schon vorhandener Daten, ist bei dieser App nicht erforderlich. Diese erfolgt automatisch während des Schreibvorgangs, wobei auch eine Warnung beim Überschreiben eines eventuell schon benutzten TAGs erfolgt. Je nach verfügbarer Speichergröße kann optional sogar ein Kontaktfoto mit abgespeichert werden. In der Datenauswahl Ansicht ist es deshalb sinnvoll, den TAG kurz zu aktivieren (mit dem TAG das Smartphone berühren), um den verfügbaren Speicherplatz zu ermitteln. Die Nachrichtengröße an sich, wird dabei permanent am oberen Bildschirmrand angezeigt und aktualisiert. Ist der verfügbare Speicher nicht ausreichend für die gewählte Nachrichtengröße, gilt es den Datensatz mit Hilfe der Auswahl Checkboxen weiter einzuschränken. Ein Beschreiben mit

Überkapazität ist hier nicht möglich und auch aus Gründen der Datenintegrität zu vermeiden.

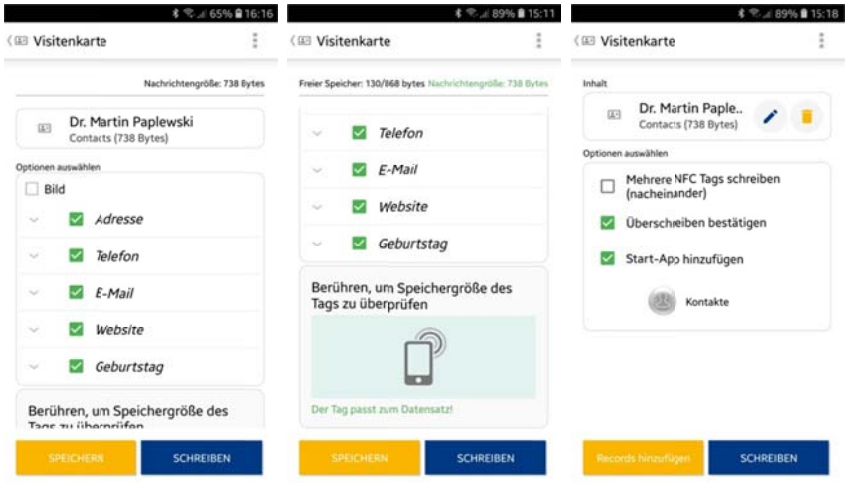


Abb. 16) smarte-Visitenkarte mit NFC

Nachdem die Datensatzgröße zum Speicherplatz passt (grün unterlegte Byte Zahl), lässt sich die digitalisierte Visitenkarte mit der blauen Schaltfläche <SCHREIBEN> auf dem TAG speichern. Der ganze Vorgang erfolgt dabei Dialog orientiert, das bedeutet den TAG erst dann ans Smartphone anzulegen, wenn die App mit einem Meldungsfenster dazu auffordert! Ansonsten den TAG kurz aus dem Antennenfeld des Smartphones entfernen und erneut anlegen.

Optional lässt sich vor dem Beschreiben auch eine Start-App auswählen, an die bei einem späteren Lesevorgang automatisch die Daten übergeben werden. In Abbildung 16 wurde beispielsweise die systemeigene Kontakte-App hinzugefügt, wodurch ein Meldungsfenster zur App-Auswahl (Abb. 17) unterdrückt wird. Auch hier kann beim erstmaligen Scan, die ausgewählte App als Standardvorgabe für den Aktionstyp in den Systemeinstellungen festgelegt werden.

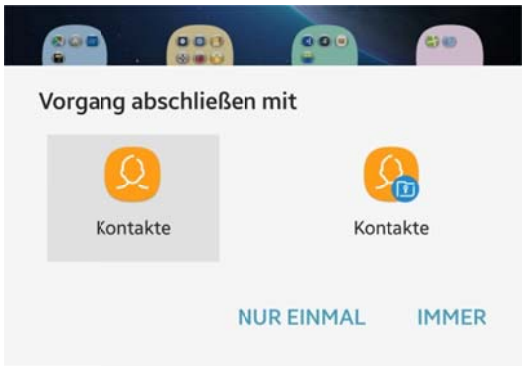


Abb. 17) Auswahldialog nach Scan der smarten-Visitenkarte

Natürlich lassen sich solche TAGs nicht nur auf Visitenkarten verwenden, sondern können auf beliebige persönliche Objekte aufgebracht, auch zum schnellen Kontaktdatenaustausch in Restaurants oder Bars benutzt werden. Da es im Ermessen des Anwenders liegt, welche und wieviel Daten abgelegt werden, erscheint auch die aktuelle Anwendung zur Kontaktnachverfolgung während der Corona Pandemie, beispielsweise im Gastgewerbe sinnvoll. Um dabei seine Daten gegen Manipulation zu schützen oder gar das Überschreiben bzw. Löschen des TAGs zu verhindern,

empfiehlt sich bei Applikationen im öffentlichen Raum einen Passwort- und/oder Sperrschutz anzulegen. Im Hauptmenü unter <Schützen> finden sich in der App dazu die drei Funktionen Schreibschutz, **Passwortschutz** und **Sichern** (Abb. 18). Obwohl sich aus den Beschreibungen eigentlich direkt die **Schreibschutz Funktion** anbieten würde, **empfiehlt sich** diese Option **nicht**, da sie die weit verbreiteten Chiptypen MIFARE Ultralight und NTAG Familie nach der Aktion unbrauchbar machen kann und keinen ausreichenden Schutz liefert. Beim Schreibschutz handelt es sich in diesem Fall nur um eine sogenannte Soft-Protektion, bei der das Schreibschutz Status Bit auf Protokollebene (im Capability Container) gesetzt wird. Trotz aktiviertem und auch funktionierendem Schreibschutz, kann der Datenspeicher aber immer noch vollständig gelöscht werden. Bei den beiden vorher genannten Chiptypen ist der Schreibschutz zudem irreversibel und kann nicht rückgängig gemacht werden. Nach Verwendung der Löschfunktion, ist ein so geschützter TAG dann zwar leer, aber immer noch schreibgeschützt und damit für die weitere Verwendung unbrauchbar.

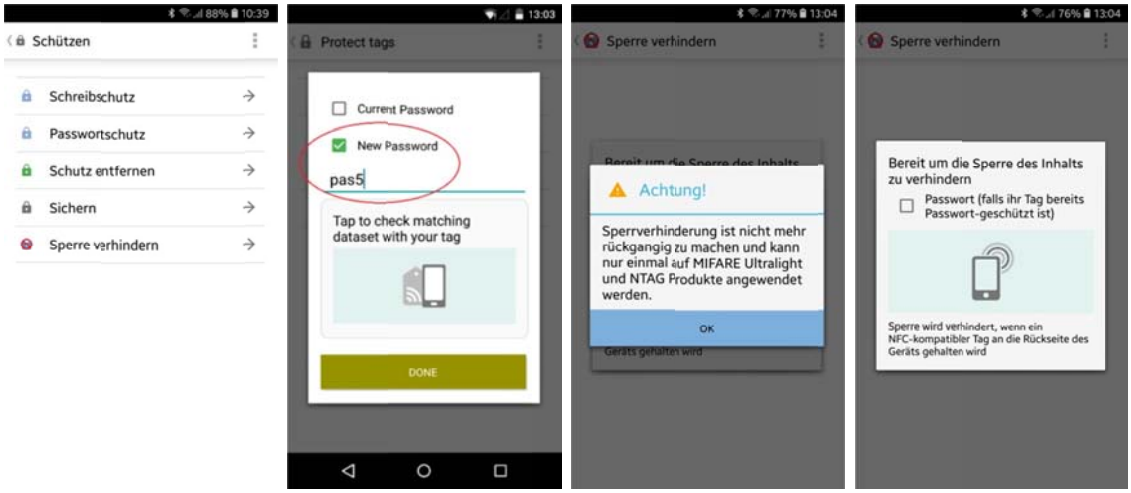


Abb. 18) Auswahloptionen zum Schützen eines TAGs

Für einen optimal geschützten TAG wird von NXP eine Kombination aus Passwortschutz mit anschließender Blockierung der Sperrfunktion <Sperre verhindern> empfohlen. Hierbei wird zunächst der Datenspeicher durch ein Passwort vor dem Überschreiben geschützt und anschließend eine **irreversible Deaktivierung** der Vollsperrung vorgenommen. Etwas unglücklich formuliert ist dabei die deutsche Übersetzung von „Lock TAG“ als <Sichern>, besser angebracht wäre hier Sperren. Mit dem von NXP vorgeschlagenen Ansatz, wird also eine mutwillige Sperrung durch Dritte verhindert, gleichzeitig aber das Beschreiben des TAGs, bei Kenntnis des richtigen Passworts weiter erlaubt. Dieses Vorgehen empfiehlt sich immer dann, wenn die abgelegten Daten später nochmals überarbeitet werden sollen. Allerdings besteht der Passwortschutz nur aus maximal vier alpha-numerischen ASCII Zeichen, sodass mit genügend Elan und Energie auch eine „Brute-Force“ Attacke zum Erraten des Passwortes möglich erscheint.

Für NFC-TAGs deren Inhalt nicht mehr geändert werden muss, bietet sich deshalb die Hardware Sperre unter dem Menüpunkt <Sichern> an. Auch diese irreversible Funktion lässt sich nicht mehr rückgängig zu machen und verwandelt den TAG, in eine „read-only“ Version mit ausschließlichem Lesezugriff. Technisch gesehen, werden solche irreversiblen Funktionen in speziellen Speicherbereichen als OTP-Zonen (one time programmable) ausgebildet, die direkt beim ersten

Schreibzugriff ausbrennen (z.B. burn-out Diode). Durch die erhöhte Spannung beim Schreibvorgang, wird die Schutzdiode einer solchen Zelle also auch wirklich physikalisch zerstört!

Nach diesem Exkurs über unterschiedliche Schutzmöglichkeiten bei NFC-TAGs, geht unser Hauptaugenmerk wieder in Richtung Anwendungsmöglichkeiten einfacher Applikationen im täglichen Gebrauch. Die elektronische Visitenkarte war ja schon ein erster Schritt. Gerade zu Marketingzwecken wäre es doch für Betriebe mit Ladenlokal und Onlineshop interessant, den Link zur Webseite mit Standortkoordinaten zu verknüpfen, um Kunden zu ermöglichen bestellte Waren direkt dort abzuholen.

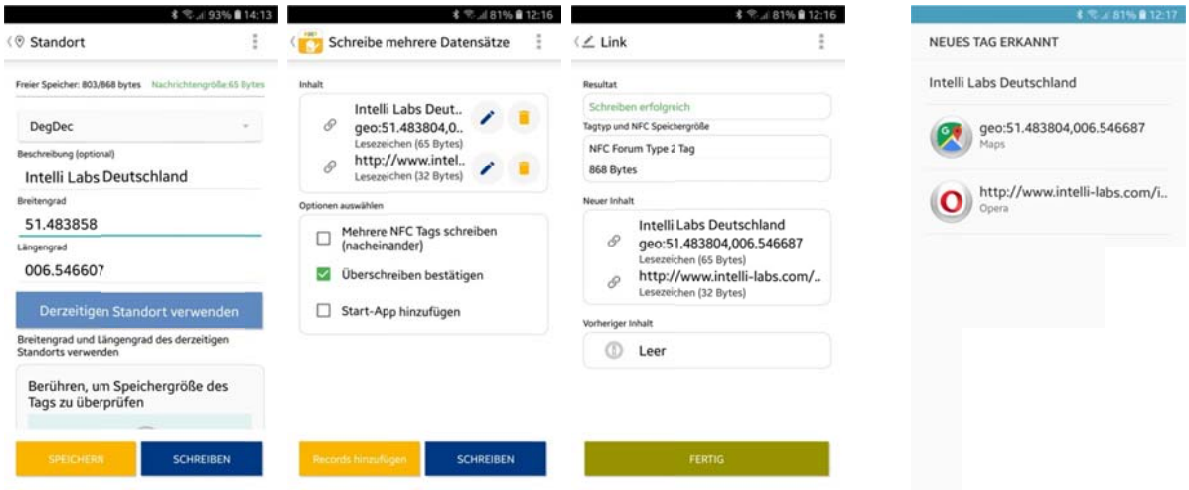


Abb. 19) mehrere NDEF-Aktionen (Link & Geodaten) auf TAG schreiben, mit Auswahlfenster nach Scan

Dies gelingt recht einfach, indem man nach Abbildung 19 mit der Schaltfläche <Records hinzufügen> vor dem eigentlichen Schreibvorgang weitere Datensätze (Aktionen) hinzufügt. Im Beispiel wurde der Standort dem Weblink angehängt. Nach dem Scan eines solch programmierten TAGs erscheint ein Auswahlfenster, in dem sich wahlweise die gewünschte Aktion ausführen lässt.

TIP

Datensätze lassen sich auch an einen schon beschriebenen TAG anhängen, solange dieser nicht gesperrt ist und der Speicherplatz ausreicht. Dazu nach dem Einlesen die Schaltfläche <Datensatz bearbeiten> + <Records hinzufügen> wählen.

Seit der Corona Pandemie nutzen immer mehr Verbraucher **kontaktlose Bezahlmöglichkeiten**. Insbesondere für kleinere und mittlere Unternehmen sowie für Selbstständige, die einen eigenen Laden oder Gastronomiebetrieb betreiben, stellt dies oftmals eine technische und kostenintensive Herausforderung dar. Als einer der weltweit größten Zahlungsdienstleister, hat auch PayPal diesen Trend erkannt und demzufolge Ende 2020 seine PayPal QR-Barcode Lösung in Deutschland vorgestellt. Der Aufwand beschränkt sich dabei auf den Ausdruck eines spezifischen QR-Codes, der sich unter dem zugehörigen PayPal Verkäufer Account generieren und herunterladen lässt. Dieser

Ansatz ist gerade für die oben genannte Zielgruppe bestens geeignet, um einen kontaktlosen Bezahlvorgang anbieten zu können. Einzige Voraussetzung ist allerdings, dass die entsprechende PayPal App auch kundenseitig auf dem Smartphone installiert sein muss. In der App wird der QR-Code dann gescannt, der Verkaufspreis eingetragen und anschließend die Zahlung ausgeführt. Da es nichts gibt, was sich nicht noch verbessern lässt, wird nun eine Lösung vorgestellt, wie sich das **PayPal QR-Code Verfahren, mit einem zusätzlichen NFC-TAG ergänzen** und „aufpimpen“ lässt. Hauptvorteil hierbei, **auf die PayPal App samt QR-Code kann komplett verzichtet werden**. Der Bezahlvorgang ähnelt eher dem bekannten Online Shopping Verfahren mit kontaktloser Ausführung. Wie bei allen kontaktlosen Bezahlmethoden mittels Smartphone (Apple Pay usw.), ist übrigens auch hier eine Internetverbindung zwingend erforderlich! Eine schlechte Netzverbindung setzt dem Ganzen dann die Grenze.

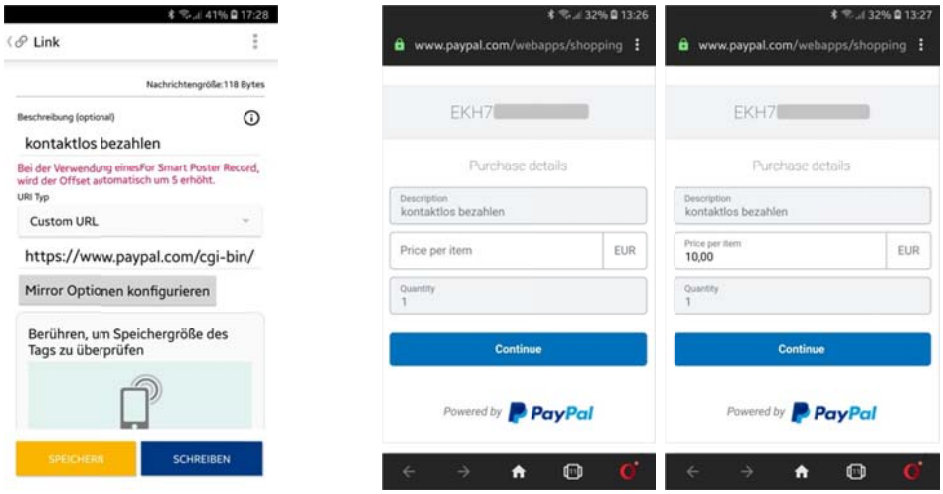


Abb. 20) kontaktloses Bezahlen für Kunden mit eigenem PayPal Link ermöglichen

Der denkbar einfachste Weg, den eigens von PayPal generierten QR-Code über den Befehl <QR Code kopieren> auf den TAG zu schreiben (Abb. 15) funktioniert dabei nicht, da der Barcode innerhalb der PayPal App gescannt werden muss. Wer es trotzdem probieren möchte, landet beim Scan des TAGs nur auf die Downloadseite der PayPal App in den Stores. Zum Programmieren des TAGs erzeugen wir uns stattdessen einen eigenen „**Jetzt Kaufen**“ Button, der eigentlich für den Einsatz auf Webseiten vorgesehen ist. Dazu im PayPal Konto unter dem Menüpunkt <Einstellungen> <Verkäufer Tools> die Option <PayPal Buttons> auswählen und anschließend im dialoggeführten Formular konfigurieren und speichern. Unter dem Menüpunkt <E-Mail> wird dann der so erstellte Button als Internet Link angezeigt, z.B.

zum Bezahlen: https://www.paypal.com/cgi-bin/webscr?cmd=_s-xclick&hosted_button_id=***1234567890***
zum Spenden: https://www.paypal.com/cgi-bin/webscr?cmd=_donations&business=***PayPal_E-Mail_Adresse***

Diesen Bezahl-Link kopieren und mit der **NFC-TagWriter** App als <Link> auf einen TAG schreiben (Abb. 20). Wer Spenden für gemeinnützige Zwecke auf kontaktlosem Wege sammeln möchte, kann sich die Erstellung eines Buttons sparen und direkt den obigen Spendenlink mit seiner PayPal E-Mail ergänzen und schreiben. Zweckmäßigerweise sollte der NFC-TAG dann auch auf der Rückseite des ausgedruckten PayPal QR-Code angebracht werden, um den Kunden beide Zahlungswege zu ermöglichen. Nach dem Scan des TAGs wird im Standard Webbrowser der aktuelle Zahlvorgang

angezeigt. Der Kunde ergänzt noch den Gesamtbetrag und führt den Zahlvorgang analog zum Online Shopping aus.

Eine Applikation die für einige Personengruppen sehr wichtig werden kann, soll am Ende dieses Kapitels nicht vergessen werden. Jeder der schon einmal in eine Notfalllage gekommen ist weiß, wie entscheidend oftmals eine schnelle Hilfe sein kann. Bei einem medizinischen Notfall sollte nicht erst Zeit der Helfer damit verschwendet werden, bestimmte persönliche Daten, wie etwa Blutgruppe oder Notfallkontakt(e) in den privaten Sachen zu suchen. Zwar gibt es dazu auch nützliche Apps für das Smartphone, wenn denn gerade das Smartphone auffindbar ist bzw. mitgenommen wurde, der Ladezustand ausreichend ist, der Sperrbildschirm überwunden werden kann und die betreffende App schnell ins Auge sticht. Ein entsprechend kodierter TAG an einer exponierten Stelle, z.B. als Sticker auf der Smartphone Hülle oder auf der Krankenkassen-Karte, kann in dieser Situation oftmals wertvolle Zeit sparen. Da auf einem NFC-TAG der Speicherplatz normalerweise ausreicht, könnten optional auch Organspenderdaten, Allergien und ähnliches abgelegt werden. Zudem hat der Benutzer zu jeder Zeit die Datenhoheit und kann letztendlich selbst entscheiden, welche Daten er auf den TAG schreibt.

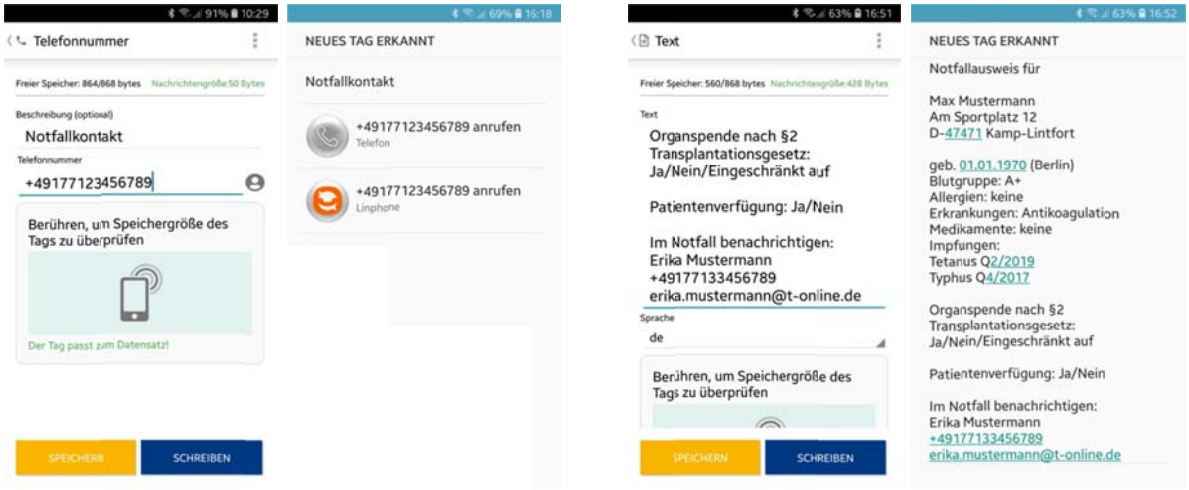


Abb. 21) Notfallkontakt & Notfallausweis mittels NFC-TAG

Um nur eine oder mehrere Telefonnummern als Notfallkontakt zu speichern, bietet sich die Auswahl <Telefonnummer> im NFC-TagWriter Menü an. Dies hat den Vorteil, dass nach Scan des TAGs optional auch der direkte Anruf ohne Nachfrage durchgeführt werden kann. Dazu im Einstellungsmenü der App unter Ereignishandhabung, die Aktion für Telefonnummer von <Anzeigen> auf <Starten> ändern.

Möglich ist aber auch die Erstellung eines NFC-TAGs als eigener Notfallausweis mittels der Menüauswahl <Text> Modus. Wie das Beispiel in Abbildung 21 zeigt, sind hiermit selbst größere Datensätze möglich. Die Formatierungs- und Gestaltungsmöglichkeiten sind zwar eingeschränkt, trotzdem werden beim Einlesen, bestimmte Formatierungsstandards automatisch erkannt und mit Aktionen hinterlegt sowie farblich hervorgehoben. Im Beispiel sind die beiden letzten Einträge richtig als Telefonanruf und E-Mail Adresse verknüpft, während alle Zahlen dabei grundsätzlich immer als Telefonnummern behandelt werden. Diese kleine Einschränkung beeinträchtigt den

Informationsgehalt aber in keiner Weise und ist ehe unter der Rubrik Schönheitsfehler abzulegen. Natürlich kann man die Informationen auch noch weiter ausbauen. Beispielsweise durch Internet-Links auf eigene Cloudspeicher, um direkt eine Patientenverfügung anzeigen zu lassen. Ebenfalls sind mit der geo: Kennzeichnung (Abb. 19) direkt Ortskoordinaten mit einer Karten-App ausführbar. Laut Speicherberechnungsanzeige sind mit dem Beispielsdatensatz zudem erst 50% des zur Verfügung stehenden TAG Speichers belegt, so dass genügend Platz für eigene Experimente vorhanden ist.

Gerade auch bei Großveranstaltungen oder mehrtägigen Festivals werden oftmals schon digitale Einlasssysteme verwendet und die zugehörigen Karten oder Armbänder an die Besucher verteilt. Erfolgt die Einlasskontrolle dabei kontaktlos, ist die Chance groß, dass ein NFC-TAG „versteckt“ eingebaut wurde. Ein Beispiel aus der Deutsch-Niederländischen EUREGIO Grenzregion zeigt dazu Abbildung 22. Auf dem Parookaville Festival 2016 in Weeze, wurden Armbänder mit eingenähten NFC-TAG ausgegeben und beim Eintrittsscan kontaktlos die TAG-ID Nummer registriert. Der vorhandene TAG Speicher blieb allerdings unbenutzt und hätte sich hervorragend zum Abspeichern von Notfalldaten oder ähnliches geeignet. Interessanterweise hatte auch im Freundeskreis, keiner je etwas von NFC oder einer kontaktlosen RFID-Technologie gehört, wobei auch niemanden die entsprechende Funktion mit NFC-Icon auf dem Smartphone aufgefallen war. Vielleicht kann dieses Werk zukünftig etwas zur Aufklärung diesbezüglich beitragen.

Abb. 22) Armband mit eingenähtem NFC-TAG als Eintrittsausweis

1.4.5 smart-CAR Applikationen

Auch im Bereich der Privatfahrzeuge, bietet die NFC-Technologie einige interessante Möglichkeiten um seinen Alltag insgesamt etwas „smarter“ zu gestalten. In Anlehnung an das vorige Kapitel starten wir zunächst mit einer einfachen Applikation als Einführung. Die Idee hierzu kam dem Autor an der Tankstelle, bei der unbefriedigenden Suche nach dem richtigen Reifendruck für eine neue Bereifung. Je nach Fahrzeugmodel sind die zugehörigen Aufkleber an den unterschiedlichsten Stellen angebracht. Bei deutschen Modellen finden sie sich vornehmlich auf der Innenseite der Tankklappe. Aufgeführt wird allerdings nur der Reifendruck, der werksseitig vorgesehenen Standardbereifung, mitunter auch für unterschiedliche Beladungszustände. Hat man dagegen eine andere Reifengröße konfiguriert oder die Reifenmarke gewechselt, sind teilweise andere Werte für die optimalen Fahreigenschaften erforderlich. So sind viele Reifenschäden die Folge eines falschen Luftdrucks. Zu wenig Luft im Reifen verlängert den Bremsweg und verschlechtert das Fahrverhalten bei Aquaplaning. Außerdem erwärmt und verformt sich der Reifen stärker, was ihn beschädigen kann. Entscheidend ist auch der Einfluss auf den Kraftstoffverbrauch, weil ein geringer Luftdruck den Rollwiderstand erhöht und damit auch die Spritkosten. Wer allerdings aus Sparsamkeit den Reifendruck jetzt zu hoch wählt, erhöht durch weniger Bodenhaftung bei höherem Abrieb gleichzeitig auch den Reifenverschleiß, was durch eine geringere Laufleistung belohnt wird. Bei sportlicher Fahrweise und in den Wintermonaten empfehlen die Reifenhersteller dagegen eine Druckerhöhung um 0,2 Bar, um Luftdruckschwankungen besser auszugleichen. Wichtig ist, der Reifendruck wird immer für den kalten Reifen angegeben, wobei die Werte den Relativdruck darstellen, also den zu zugegebenen Druckaufschlag. Physikalisch gesehen, bedeutet ein Reifendruck von 2,5 Bar, dann einen Absolutdruck im Reifen von ca. 3,5 Bar (Druckangabe plus Atmosphärendruck). Auch bei einem absolut dichten Reifen, schwankt dabei der Reifendruck mit dem Wetter, hervorgerufen durch einen veränderten Atmosphärendruck sowie Temperaturunterschiede. Demzufolge wird eine regelmäßige Reifendruck Kontrolle (~14 Tage), insbesondere auch bei den schwereren Elektroautos immer wichtiger.

TIP

Um die Abhängigkeit des Reifendrucks von der Außentemperatur zu verringern, empfiehlt sich eine Erstbefüllung mit einem sogenannten Reifengas beim Händler. Das aus reinem Stickstoff bestehende Gas, enthält weder Wasser (Luftfeuchtigkeit) noch Sauerstoff und mildert so auftretende Druckschwankungen. Wie entscheidend sich selbst kleinste Reifendruckschwankungen auf die Performance auswirken, kann man hautnah bei den Rennen der Formel 1 beobachten.

Nach diesem Exkurs in die durchaus lehrreiche Reifentechnologie, stellt sich jetzt mehr und mehr die Frage, was das ganze Thema eigentlich mit NFC zu tun hat. Nun, wäre es nicht nützlich die Reifendaten immer direkt am Objekt, also am zugehörigen Rad zu haben?

Ein Vorschlag dazu zeigt Abbildung 23. Hier wurde ein NFC-TAG in die Radnabenabdeckung eingeklebt, welcher sich auch nach der Montage noch einfach mittels Smartphone direkt am Rad auslesen lässt. Die Radnabenabdeckung sollte dabei natürlich aus Kunststoff oder anderen nicht

elektrisch leitfähigen Materialien bestehen. Zusätzlich empfiehlt es sich, den TAG noch gegen Schmutz und Korrosion, beispielsweise mit einer Silikonschicht abzudichten. Auch in diesem Beispiel wurde der NFC-TAG mit Daten im freien Textformat (NFC-TagWriter App) beschrieben. Neben den Druckwerten, wäre beispielsweise noch die Aufnahme des Montagedatums samt Kilometerstand hilfreich, um die Laufleistung eines Reifensatzes auswerten zu können.

Abb. 23) Radnabenabdeckung mit NFC-TAG, Abfrage der Reifendaten am Rad

Dieser Ansatz ließe sich selbstverständlich noch „smarter“ gestalten und weiter ausbauen. Durch die Integration einer RFID-Antennenspule am Reifenbefüllungsventil sowie dem Einbau eines NFC-Readers im Druckmessgerät, könnte der passende Soll-Druck automatisiert digital eingestellt werden. Da häufig auch schon der eigentliche Befüllvorgang automatisch abläuft (Ist/Soll-Wert Abgleich), wäre dann der komplette Vorgang vollständig digitalisiert. Sollte zufälligerweise ein Hersteller von Luftdruckfüllständen noch weitere Informationen wünschen, kann er dazu gern den Autor kontaktieren.

Wie schon öfters erwähnt, unterstützt die NFC-Technologie auch die ereignisgesteuerte Ausgabe von programmierbaren Steuerbefehlen. Dieses Verfahren ist komplexer, als die bislang beschriebenen Möglichkeiten und schon eher mit einer Art von Software Programmierung vergleichbar. Mit der nachfolgend vorgestellten Applikation im smart-CAR Sektor, wird dieses Verfahren benutzt, um ein Smartphone nach Einlegen in die Autohalterung, automatisch in einen benutzerfreundlichen Auto-Modus zu versetzen. Dazu wird zunächst jedoch eine andere App namens „**NFC Tools**“ benötigt, die sowohl für Android als auch iOS in den Stores frei verfügbar ist (Abb. 24). Die in den Screenshots dargestellte Pro-Version ist dagegen kostenpflichtig, besitzt dafür aber einen erweiterten Funktionsumfang. Sollte man sich später für den Kauf der Pro-Version entscheiden, empfiehlt sich die „stand-alone“ Version direkt von der französischen Entwicklerseite herunterzuladen. Diese sogenannte SE-Version, hat keine Google oder Apple Store Bindung und unterliegt somit auch nicht bestimmten Restriktionen infolge geänderter Geschäftsbedingungen (z.B. beim SMS-Versand).

Mit „**NFC Tools**“ lassen sich alle Grundfunktionen zum Lesen, Schreiben und Programmieren eines TAGs durchführen. Für die automatische Abarbeitung gespeicherter Befehlssequenzen auf einem beliebigen Smartphone, ist dagegen eine schlanke, speziell optimierte „**NFC Task**“ App notwendig.

Die App wird während der Installation, als eigenständiger Systemdienst gestartet. Ohne eigene Benutzeroberfläche, reagiert sie anschließend nur noch auf bestimmte NFC Ereignisse (z.B. TAG erkannt). Sind programmierte Steuerbefehle mit korrekter Kodierung in den gelesenen Daten vorhanden, so werden diese im Hintergrund auf Systemebene automatisch ausgeführt. Angenehm fällt auf, dass sich die zulässigen App Berechtigungen zum Zugriff auf Systemfunktionen, je nach Anwendungsfall beliebig einschränken oder erweitern lassen. Grundkenntnisse in der System Konfiguration eines Smartphones werden aber vorausgesetzt!

Abb. 24) NFC Tools für Android und iOS – Download Links
https://play.google.com/store/apps/details?id=com.wakdev.wdnfc
https://apps.apple.com/us/app/nfc-tools/id1252962749

Screenshots in der nachfolgenden Beschreibung beziehen sich ausschließlich auf die App „**NFC Tools**“. Die zur Ausführung separat benötigte „**NFC Task**“ App kann ebenfalls über die Download Links der Abbildung 24 bezogen werden.

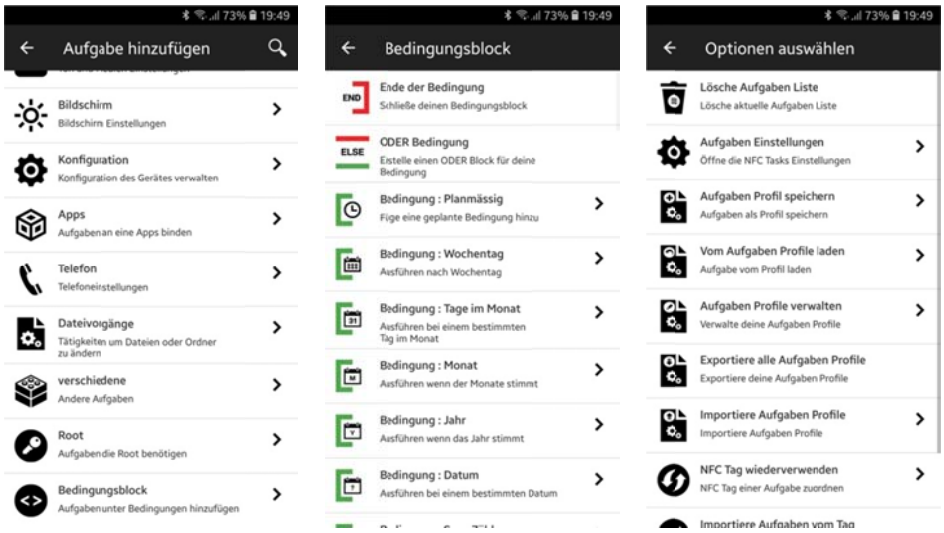


Abb. 25) NFC Tools für Android und iOS – Download Links

Nach dem ersten Start der App fällt dem Anwender direkt die Komplexität der angebotenen Funktionen ins Auge. Neben den Standardfunktionen <Lesen> und <Schreiben>, finden sich unter dem Menüpunkt <Andere> die Sonderfunktionen zur TAG Verwaltung. Für unsere Applikation ist aber die Option <**Aufgaben**> entscheidend (Abb. 25). Im Kontext der App sind Aufgaben gleich zusetzten mit Befehlssequenzen, die blockweise zusammengestellt werden. Blöcke können hier ebenso von einzelnen, aber auch verschachtelten IF ELSE END Bedingungen eingeschlossen sein. Allein die Anzahl von 63 zur Verfügung stehenden unterschiedlichen Bedingungsblöcken in der Pro-Version macht klar, dass die Programmierung kein Selbstläufer ist, sondern etwas Beschäftigungszeit

erfordert. Unter der Schaltfläche <Aufgaben> <Mehr Optionen> <Aufgaben Einstellungen> finden sich zudem weitere Konfigurationsmöglichkeiten zum Fine Tuning während des Programm Ablaufs. Neben den direkten Zugriff auf die Berechtigungseinstellungen, lassen sich unter anderem eigene Benutzer Variablen definieren und Debug Benachrichtigungen zur Fehlersuche festlegen. Eine auch für unsere Applikation wichtige Einstellung verbirgt sich unter dem Punkt <Sonstiges>. Da das Smartphone während der Fahrt normalerweise ständig in der Ablage liegt, befindet sich somit auch der NFC-TAG permanent im Detektionsfeld. Es gilt also durch geschickte Programmierung, ein ständiges Wiedereinlesen des TAGs, in Form einer Endlosschleife zu verhindern. Dazu bietet sich als erste Teillösung, die Einstellung einer Verzögerungszeit von mindestens 30 Sekunden an. Der Ausschnitt des Beispielprogramms nach Abbildung 26 zeigt einen weiteren Lösungsansatz. Im ersten Blockbefehl wird hier direkt der Bluetooth Verbindungsstatus vom Smartphone mit dem Mediacenter des Fahrzeugs überprüft. Wurde die Verbindung schon hergestellt (True), wird eine weitere Ausführung sofort beendet. Allerdings gibt es bei diesem Lösungsweg auch einen Nachteil, den der aufmerksame Leser sicherlich schon bemerkt hat. Damit die Aufgaben beim ersten Scan überhaupt ausgeführt werden, muss entweder Bluetooth abgeschaltet sein, oder das Smartphone vor dem Einschalten der Zündung in die Halterung gelegt werden. Ansonsten besteht die Möglichkeit, dass sich das Smartphone schon vor dem TAG Scan mit dem Mediacenter koppelt; je nachdem welcher der beiden Tasks (Bluetooth oder NFC) gerade priorisiert läuft. Aufgrund der Vielzahl an möglichen Bedingungsblöcken, lassen sich sicherlich noch weitere Trigger finden, die dieses Problem umgehen. Der Vollständigkeit halber sei erwähnt, dass der anschließende Bedingungsblock in Abb. 26, mittels Abfrage der IMEI Nummer die Ausführung auf ein spezielles Smartphone begrenzt.

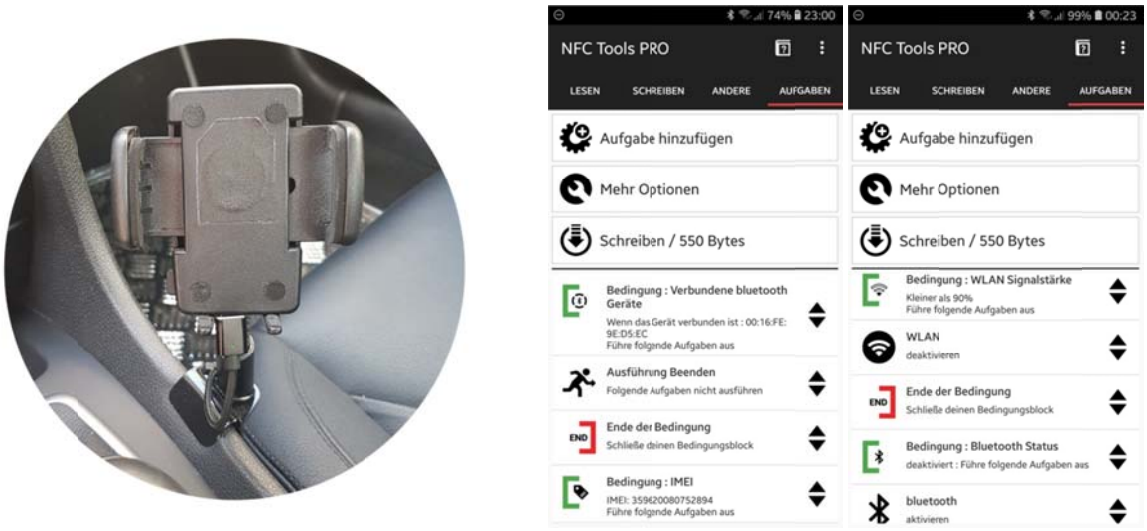


Abb. 26) smart-CAR Applikation mit NFC-TAG in der Handy-Halterung und NFC Tools App

Übrigens lassen sich bei geschickter Ausrichtung des NFC-TAGs auf einer Ladeschale, sowohl die NFC-Funktion, als auch das drahtlose Laden nach dem QI-Standard gleichzeitig ausführen. Prinzipiell sollte damit die aufgezeigte smart-CAR Applikation, auch bei Fahrzeugen, mit von Werk aus integrierten drahtlosen Ladeschalen funktionieren. Warum zwei, an sich konkurrierende Funkstandards, dennoch parallel ohne Störung arbeiten, wird aus dem folgenden Kapitel ersichtlich.

2. RFID Technologie

2.1 Grundlagen der Technologie

Zuallererst steht die Abkürzung RFID für „Radio Frequency IDentification“. Frei übersetzt also der Identifizierung damit gekennzeichneter Objekte, mittels hochfrequenter Funkwellen geringer Leistung aus einem spezifischen Frequenzband. Im Wesentlichen deckt diese Technologie zunächst den gleichen Applikationsbereich, wie der weit verbreitete Barcode, ab. Die RFID besitzt aber einige einzigartige Vorteile und Eigenschaften, womit sie durchaus als Nachfolge-Technologie zu existierenden Barcode und Magnetstreifen Lösungen anzusehen ist.

RFID Vorteile gegenüber Barcode

- kein direkter Sichtkontakt (line of sight) notwendig
- Lese- und Schreibfunktionalität vorhanden, dadurch wiederbeschreibbar
- unterschiedliche Technologien und Speichergrößen verfügbar
- Sicherheitsmerkmale mit Datenschutzfunktion integriert
- werksseitig feste, weltweit eindeutige ID-Nummer
- einfacher, kostengünstiger Aufbau
- keine eigene Stromversorgung nötig (passive Transponder)
- auch unter extremen Umgebungsbedingungen einsetzbar (XTC-ID)

Die RFID-Technologie basiert auf der Übertragung von Daten mittels elektromagnetischer Felder – also drahtlos per Funk. Informationen über ein Objekt werden auf einem Datenträger gespeichert, bekannt als Transponder (abgekürzt TAG), der am Objekt befestigt oder eingebettet wird. Dieser Transponder besteht aus einer Antenne sowie einem Chip, auf dem die Daten abgelegt werden. Diese Informationen können entweder aus objektbezogenen Daten oder noch einfacher, nur aus einer eindeutigen Seriennummer mit Verlinkung zu den eigentlichen Daten in einer Datenbank, bestehen. Analog zum Barcode wird dieser Datenträger direkt mit dem Objekt fest verbunden und ermöglicht es so, die Informationen jederzeit zu lesen oder wenn gewünscht zu ändern. Dazu kommuniziert der TAG mit einer Lese- / Schreibstation, allgemein als Reader bezeichnet (Abb. 27).

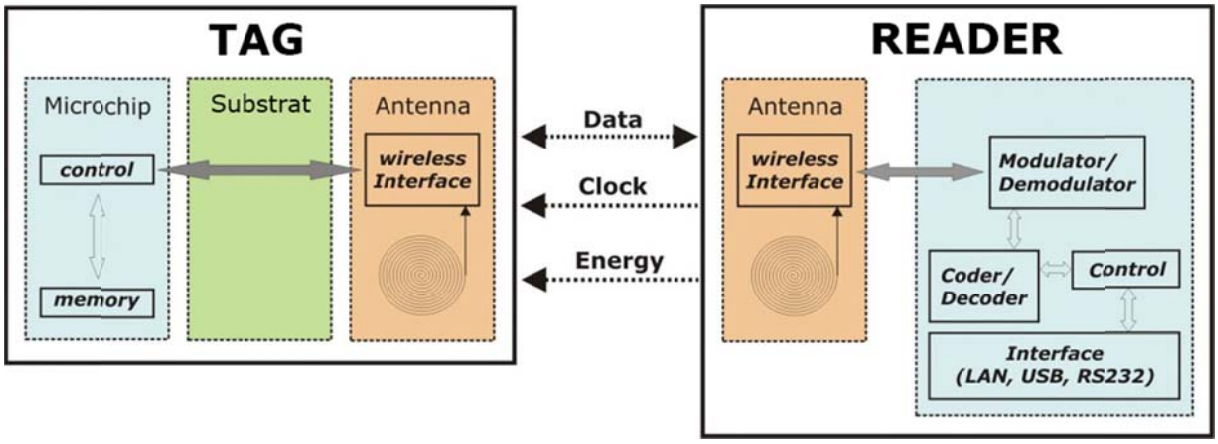


Abb. 27) automatische Identifikationsmethode mittels hochfrequenter Funkwellen geringer Leistung (1-2 Watt)

Etwa 95% aller verwendeten Tags sind passive Typen, die keine eigene Stromversorgung aufweisen. Sie werden mit Energie versorgt, welche durch ein Hochfrequenzfeld (HF-Signal) in der Antenne induziert wird. Für spezielle Anwendungen stehen heute aber auch aktive Tags mit interner Stromquelle und/oder eingebetteter Sensorschnittstelle (für Temperatur, Druck etc.) zur Verfügung. Die klassische Einteilung nach –aktiven oder passiven– Typen verschwimmt dabei zukünftig immer mehr. Optimierte Fertigungsprozesse erlauben die Herstellung immer leistungsfähigerer (integrierte Sensoren) und gleichzeitig extrem energiesparender Silizium-Chips, die sowohl drahtlos wie auch extern mit Energie versorgt werden können. Damit sind gerade in der Medizintechnik neue innovative Applikationen möglich. Um die geforderte hohe Lebensdauer zu gewährleisten, werden bei unserer XTC-ID Technologie aber aktuell ausschließlich passive TAGs verwendet.

Während des Betriebs sendet das Lesegerät (Reader) permanent und in kurzen Zeitschleifen elektromagnetische Wellen aus. Eine solche zeitgesteuerte Abfragefunktion wird in der Technik häufig auch als „polling“ bezeichnet. Beispielsweise beträgt die Poll-Rate beim XTC-ID Reader dreimal pro Sekunde (3 Hz), wodurch eine schnelle Objektdetektion erzielt wird. Die TAG-Antenne ist darauf abgestimmt, diese Wellen zu empfangen. Der TAG identifiziert sich selbst, sobald er ein Signal in der Hochfrequenzübertragung von einem Lesegerät empfängt. Wenn also ein TAG, ein von einem kompatiblen Lesegerät erzeugtes Feld durchläuft, überträgt es die gespeicherten Informationen zurück an das Lesegerät und identifiziert so das Objekt. Das Vorhandensein eines TAGs moduliert dabei das HF-Feld und wird somit ebenfalls vom Lesegerät erkannt. Eine geringfüge Ansprechverzögerung kommt dadurch zustande, dass der TAG beim Eintritt in das vom Lesegerät erzeugte HF-Feld, zunächst einen kleinen Teil der HF-Energie zur eigenen Stromversorgung absorbieren muss. Erst wenn ausreichend Energie aufgenommen wurde, beginnt der eigentliche Kommunikationsprozess, entweder durch Amplituden- *(Amplitude Shift Keying)* oder Frequenz- *(Frequency Shift Keying)* oder Phasenmodulation *(Phase Shift Keying)* des HF-Trägersignals (Abb. 28). Das Lesegerät demoduliert anschließend die von der TAG-Antenne empfangenen Signale und decodiert die Daten zur weiteren Verarbeitung und Ausgabe.

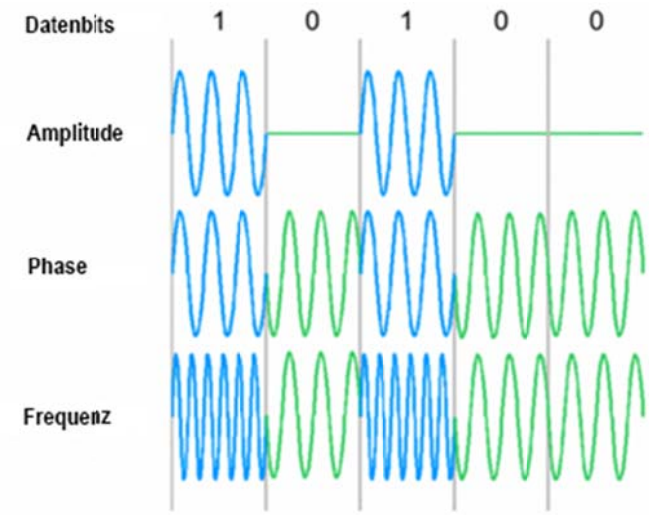
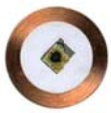
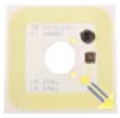


Abb. 28) typische Modulationsarten für Funkübertragungen

2.2 RFID Frequenzbereiche & Standards

Seit ihrer ersten kommerziellen Einführung Anfang der 90er Jahre, hat die RFID-Technologie mehrere Entwicklungsschübe vollzogen und sich deutlich weiterentwickelt. Wie bei anderen Funktechnologien (z.B. Mobilfunk), zeigt sich auch hier eine Evolution hin zu immer höheren Frequenzbereichen mit fortschreitender Miniaturisierung der elektronischen Bauelemente, verbunden mit einer immer einfacher werdenden Antennenstruktur. Historisch bedingt teilt man unterschiedliche RFID-Technologien, deshalb am besten nach ihren Frequenzbändern in drei Hauptklassen ein. Niedrige Frequenzen sind dann gleichbedeutend mit einer älteren, aber nicht unbedingt weniger leistungsfähigeren Technologie. Eine Übersicht der jeweiligen Vor- und Nachteilen zeigt nachstehende Tabelle 1.

	**Low-frequency (LF):** 125 bis 134.2 kHz Zutritt-Systeme, Tier ID, Automobil Funkschlüssel + störunempfindlich, einsetzbar in rauen Umgebungen & auf Metalloberflächen + exzellente Materialdurchdringung beim Lesen, Lesereichweite bis 50 cm – geringe Lesegeschwindigkeit & Speichergröße, keine Mehrfacherkennung – aufwendig gewickelte Antennenspulen, proprietäre Technik, relativ teuer
	**High-frequency (HF):** 13.56 MHz *(ISO15693, ISO14443, ISO18000-3)* Smarte Etiketten, IoT, Logistik, Chipkarten, NFC etc. + ISO-Standard, hohe Lesegeschwindigkeit & Speichergröße, Sicherheitsfunktionen + gute Materialdurchdringung, Mehrfacherkennung möglich, relativ preiswert – schlechte Performance auf Metalloberflächen oder durch wässrige Medien – Lesereichweite < 10 cm (bei NFC), sonst typisch < 1 m
	**Ultra-high-frequency (UHF):** 850 MHz bis 960 MHz *(ISO18000-6, EPC Gen2)* Logistik, Produktlokalisierung, Gepäckverfolgung + Lesereichweite > 3 m, höchste Lesegeschwindigkeit, Speichergröße, günstiger Preis + „bulk“ Mehrfacherkennung, einfacher Aufbau mit Dipolantenne – hohe Störempfindlichkeit, geringe Materialdurchdringung, relativ teure Lesegeräte – keine weltweit einheitlichen Frequenzen & Sendeleistung

Tab. 1) Eigenschaften der RFID-Typen unterteilt nach Frequenzbereich

Aus der LF-Technologie heraus, hat sich ab 2008 durch einen Zusammenschluss namhafter Hersteller als WPC (Wireless Power Consortium), ein Standard zum drahtlosen Laden „Wireless Charging“ von mobilen Endgeräten entwickelt. Primär steht hier allerdings nicht eine Datenübertragung, sondern die induktive Energieübertragung zwischen zwei Antennenspulen im Vordergrund. Dennoch werden kleinere Datenpakete zu Synchronisationszwecken sowie oftmals auch Ladeparameter mit übertragen. Der aktuell wichtigste Standard für die drahtlose Stromübertragung, trägt den Namen Qi (ausgesprochen „tschi“) und steht in der chinesischen Sprache für Lebensenergie oder Lebenskraft. Neben einer Leistung von bis zu 15 Watt, beinhaltet Qi zudem sicherheitsrelevante Schutzvorrichtungen und eine zuverlässige Fremdkörpererkennung, für z.B. zufällig auf der Senderspule der Ladestation geratene Objekte (Büroklammer, Schmuck usw.). In solch einem Fall darf die Ladestation nicht in Betrieb gehen, denn aufgrund der induzierten Ströme innerhalb der Metallteile würden sich die Gegenstände soweit erhitzen, dass ein Brand entstehen kann. Bei der RFID-Technologie sind dagegen die induzierten Stromstärken vernachlässigbar gering.

Im HF-Frequenzbereich bei 13.56 MHz hat sich zur selben Zeit ebenfalls ein neuer Standard für die drahtlose Nahfeldkommunikation kurz NFC „Near Field Communication“ etabliert. Dabei handelt es sich nicht um eine neue RFID-Technologie, sondern um eine Erweiterung bisheriger ISO-Standards im HF-Band. NFC zielt dabei besonders auf die einfache Ausführung von Transaktionen und Datenübertragungen oder dem Koppeln drahtloser Verbindungen über kurze Entfernungen bis 10 cm ab. Infolge der kurzen Reichweite sowie einem Punkt-zu-Punkt Kommunikationskanal, ist dabei die Datensicherheit deutlich höher als bei anderen Funkstandards. Im Vergleich zur herkömmlichen RFID, besteht die grundlegende Idee der NFC, in Verwendung nur eines elektronischen Bauteils (typischerweise im Smartphone integriert), mit dem sich dann drei verschiedene Einsatzgebiete abdecken lassen: Lese/Schreib Emulation, Karten Emulation und „Peer-to-Peer“ Kopplungen zweier Endgeräte (Abb. 29).

Abb. 29) Definierte Einsatzarten im NFC-Standard
(© 2016 EBV Elektronik, „RFID Selection Guide“)

Bei der Lese/Schreib Emulation verhält sich das mobile Endgerät wie ein herkömmlicher RFID-Reader, während ein NFC TAG den anderen Kommunikationspartner auf der Gegenseite darstellt. Dieser Modus stellt das typische Einsatzgebiet der RFID dar und wurde schon ausführlich im ersten Kapitel behandelt. Eindeutiger Vorteil bei Gebrauch der NFC ist der teilweise Wegfall, aller weiteren Hard- und Software Ausstattung, da ein kompatibles Smartphone diese Funktionalität schon vom Werk aus mitbringt. Dementsprechend hoch ist dessen Marktdurchdringung.

Eine Erweiterung im NFC Standard, stellt dagegen die Karten Emulation oder besser TAG Emulation dar. In diesem Fall nimmt das mobile Endgerät die Position eines TAGs ein, während die Gegenseite als RFID-Reader fungiert. Der Begriff Karten Emulation greift etwas zu kurz, da er aus den ursprünglich angedachten Anwendungen für das kontaktlose Bezahlen abgeleitet wurde und auf die Erzeugung einer „virtuellen“ Smartcard mittels Smartphone App beruht. Aus Kompatibilitätsgründen zu schon bestehender Hardware Ausstattung, besteht technisch kein Unterschied bei Verwendung einer „echten“ Karte oder deren Smartphone Emulation. Prinzipiell ist es aber auch möglich, alle anderen NFC-TAGs zu emulieren, solange es dessen Sicherheitsfunktionen zulassen! Dazu genügt es häufig einen vorhandenen TAG einmalig auszulesen, den Datensatz abzuspeichern und später daraus einen „virtuellen“ TAG auf dem Smartphone zu generieren.

Bei der Peer-to-Peer Kopplung zweier Endgeräte, wird dagegen komplett auf den Einsatz eines herkömmlichen NFC-TAGs verzichtet. Beide Partner im Kommunikationskanal sind gleichberichtigt und dienen gleichzeitig als Lese-/Schreibgeräte. Eine solche eins-zu-eins Punktverbindung ist analog dem bekannten Bluetooth Standard, wobei aber ein vorhergehendes Pairing entfällt. In diesem Fall wird infolge der geringen Übertragungsreichweite die Datensicherheit gewährleistet. Aktuell führt dieser Modus eher ein Schattendasein und ist ausschließlich auf Android Smartphones, unter der Bezeichnung „Android Beam“ auf Betriebssystemebene verfügbar. Android Beam dient häufig dem unkomplizierten Austausch einzelner Dateien oder Medienobjekte zwischen zwei Smartphones, durch einfache Berührung miteinander. Beide Endgeräte müssen während der Übertragung dabei in permanenten Kontakt bleiben. Für einen Transfer großer Datenmengen sind dagegen effizientere Übertragungswege, wie z.B. Bluetooth oder Wi-Fi besser geeignet.

Eine weitere Entwicklung ist hardware-seitig bei den zukünftigen RFID-Chips der TAGs zu beobachten. Neben dem rein drahtlosen RFID-Interface, wird zunehmend eine zweite, kabelgebundene Bus-Schnittstelle (I²C/SPI) implementiert. Solche „dual Interface“ TAGs erlauben damit die Kommunikation mit einem angeschlossenen Mikrokontroller bzw. externer Sensorik, auch bei nicht aktivem RF-Feld. Häufig dient der TAG dabei als Datenspeicher z.B. für Kontrollfunktionen, der bei Bedarf drahtlos über das RF-Interface extern ausgelesen werden kann, ohne die Funktionalität des Systems zu unterbrechen. Damit sind z.B. neue Anwendung im Service, wie Upload neuer Konfigurationsdaten, Auslesen von Fehlerspeichern oder Wartungsintervallen, ohne internen Eingriff direkt im laufenden Betrieb möglich. Der Einsatz extrem energiesparender Mikrokontroller erlaubt weiterhin ein „Energy Harvesting“ (Energieernte) bei angelegtem RF-Feld (Abb. 30). So können z.B. Sensoren bei Bedarf (on-demand) ausgelesen werden und benötigen dann keine eigene Energiequelle.

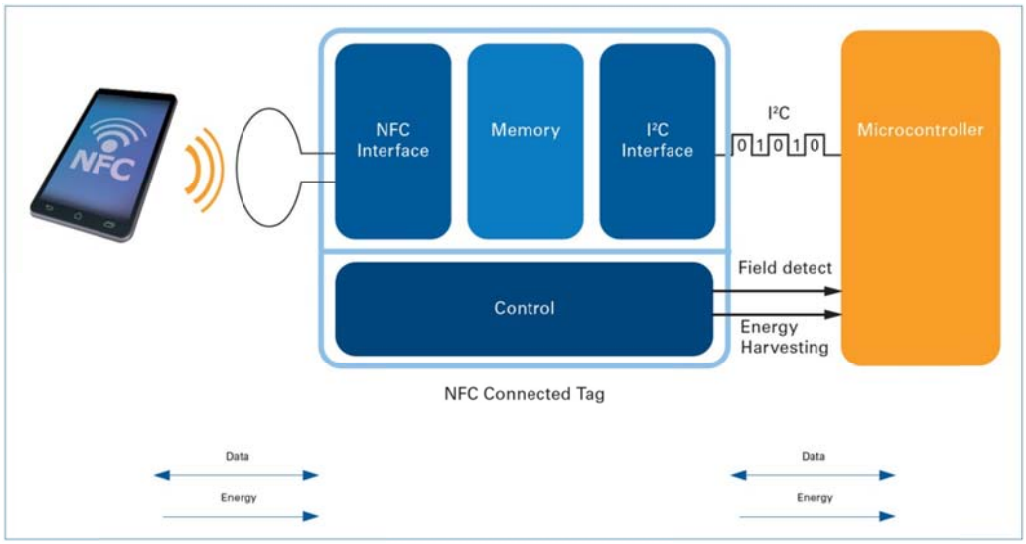


Abb. 30) Funktionsweise eines Dual Interface TAGs mit Energy Harvesting
(© 2016 EBV Elektronik, „RFID Selection Guide“)

Ein weiteres wichtiges Merkmal aller zurzeit verfügbaren RFID-Chips, besteht in einer werkseitig fest einprogrammierten, eindeutigen Seriennummer abgekürzt UID (Unique Identification Number) genannt. Wie im ersten Kapitel bereits erwähnt, ist diese vergleichbar mit der MAC-Adresse von TCP/IP basierten Netzwerkgeräten und ist wie dort, bei einer entsprechenden Byte Anzahl auch weltweit eindeutig kodierbar. Neben dem Vorteil einer eindeutigen Identifikation von so gekennzeichneten Objekten, erfolgte die ursprüngliche Einführung der UID aus technischen Gründen laut ISO/IEC 14443-3 Spezifikation. Wie in einem LAN-Netzwerk, muss auch ein RFID-Reader in der Lage sein, mehrere gleichzeitig im RF-Feld vorhandene TAGs eindeutig voneinander zu unterscheiden, um die Datensätze richtig zuordnen zu können. Aufgrund der geringen Reichweite von NFC ist dieses Problem aber hier, als praktisch wenig relevant anzusehen. Dank der Eindeutigkeit der UID ergeben sich zahlreiche Anwendungsfälle, die mit alternativen Produktkennzeichnungen (Barcodes, QR-Codes) nicht realisierbar sind.

Die aktuell verwendeten NFC-TAGs benutzen typischerweise sieben Byte zur Speicherung der Seriennummer und bieten somit Platz für eine 14-stellige Hexadezimalzahl. Das Hexadezimalsystem ist in ein in der Informatik übliches Zahlensystem zur Basis 16, bei dem aber von 0 bis F gezählt wird, anstelle von 0 bis 9, wie im allgemein gebräuchlichen Dezimalsystem. Umgerechnet ergeben sieben hexadezimale Byte als FF:FF:FF:FF:FF:FF:FF, somit eine maximal Anzahl von 72.057.594.037.927.935 möglichen Seriennummern. In der Realität ist der zur Verfügung stehende Nummernkreis allerdings etwas kleiner, da teilweise Blöcke für Hersteller oder Produktlinien reserviert werden. Daher sieht die ISO/IEC Spezifikation auch die dynamische Erweiterung der Nummernbereiche vor. Die Vergangenheit hat beispielsweise gezeigt, dass die bei den älteren TAGs verwendeten vier Byte UIDs schon vor einigen Jahren ausgegangen sind und damit größere Zahlenräume notwendig wurden. Derzeit sind folgende UID-Varianten spezifiziert und im Gebrauch:

UID Typ	Byte Folge	Hexadezimal	max. Anzahl
Single Size NUID (Non-Unique Identifier)	4 Byte	FF:FF:FF:FF	4.294.967.295

Eine vier Byte NUID kann während des gesamten Produktionszeitraums eines Chip Typs mehr als einem RFID-Chip zugeordnet werden, sodass prinzipiell mehr als ein TAG mit derselben Identifikation existiert. Die Wahrscheinlichkeit, dass zwei Chips identischer Seriennummer gleichzeitig in einer Applikation aufeinandertreffen, ist aber immer noch extrem gering. Diese Art von NUIDs ist häufig in Byte null / Bit eins (Zählweise beginnt bei null) mit UID0 = xF (hexadezimal) markiert. Für Spezialanwendungen wie beispielsweise Kreditkarten, existieren weiterhin vier Byte RID (Random Identifier) Typen. In diesem Fall wird die UID bei jedem Eintritt in ein Reader RF-Feld, durch einen Zufallsgenerator dynamisch neu erzeugt. Erkennbar sind diese an der UID0 = 0x08 Kodierung.

UID Typ	Byte Folge	Hexadezimal	max. Anzahl
Double Size UID	7 Byte	FF:FF:FF:FF:FF:FF:FF	72.057.594.037.927.935

Moderne Chips mit sieben Byte UIDs enthalten immer einen Herstellercode in der UID0, der im ISO/IEC JTC1/SC17 Dokument 5 gelistet ist (Anhang A). Ein TAG mit NXP Chip[4)] besitzt demzufolge eine UID0 = 0x04 Kodierung.

UID Typ	Byte Folge	Hexadezimal	max. Anzahl
Triple Size UID	10 Byte	FF:FF:FF:FF:FF:FF:FF:FF:FF:FF	1.2089258196146E+24

Derzeit gibt es keinen Chip, der eine UID mit dreifacher Größe verwendet. Es ist jedoch zwingend vorgeschrieben, dass jeder neue Reader Chipsatz die zehn Byte UIDs gemäß ISO/IEC 14443 unterstützt. Auch hier wird ebenfalls ein Herstellercode in UID0 kodiert.

UIDs neuerer Chiptypen werden zunehmend nach der erweiterten ISO/IEC 15693-3 Spezifikation mit 64-Bit UID (8 Byte) kodiert. Um die Verwirrung komplett zu machen, wurde dabei die Zählweise gegenüber der allgemein üblichen Bitnummerierung innerhalb eines Bytes getauscht. Die Durchnummerierung beginnt in diesem Fall beim LSB (low significant byte) mit Bit 1 und endet beim MSB (most significant byte) mit Bit 64. Dadurch gehört die UID0 nun mit zur eigentlichen Seriennummer, während der Herstellercode jetzt in UID6, direkt neben der neu eingeführten Chip Typ Kodierung UID5 zu finden ist.

MSB							LSB
64 : 57	**56 : 49**	**48 : 41**	**40 : 1**				
0xE0	0x04	0x01	werksseitige IC Seriennummer				
UID 7	UID 6	UID 5	UID 4	UID 3	UID 2	UID 1	UID 0

Tab. 2) 64-Bit (8 Byte) UID Kodierung nach ISO/IEC 15693-3

Der im XTC-ID TAG verwendet ICODE SLIX2, gehört zu den Chips neuster Generation und wurde nach dieser Spezifikation programmiert (siehe Tab. 2). Für die in Abbildung 31 als Beispiel dargestellte UID eines Chips von diesem Typ, ergibt sich mit 0x04 der Herstellercode für NXP (siehe Anhang A) sowie mit dem darauffolgenden Byte 0x01 eine ICODE SLIX Version[1)].

Abb. 31) Beispiel einer 64-Bit UID im ICODE SLIX2

3. XTC-ID Technologie

3.1 Projektidee & Aufgabenstellung

Trotz des hohen Potentials der RFID zur Kennzeichnung, Identifizierung und Nachverfolgung, ist ihr Einsatz in industriellen Anwendungen kaum verbreitet. Bis auf einige spezielle Massenmärkte z.B. in der Logistikbranche oder als Zutrittskontrolle, werden oftmals alternative Barcode Lösungen bevorzugt, deren Einsatz unter rauen Umgebungsbedingungen aber hier recht schnell an seine Grenzen stößt. Allerdings sind auch die zurzeit verfügbaren RFID-TAGs, nur eingeschränkt für derlei industrielle Applikationen geeignet. Primäres Projektziel war es deshalb, einen robusten und inerten RFID-Transponder zum langlebigen Einsatz unter extremen Umweltbedingungen zu entwickeln. Damit wäre als sekundäres Ziel, die Erfassung eines gesamten Arbeitsablaufs (Workflow), auch in Prozessschritten mit extremen Bedingungen, durch Integration dieser neuartigen TAGs möglich. Zu solchen Einsatzbereich zählen beispielsweise extrem tiefe oder hohe Temperaturen sowie korrosive Atmosphären usw. (Abb. 32).

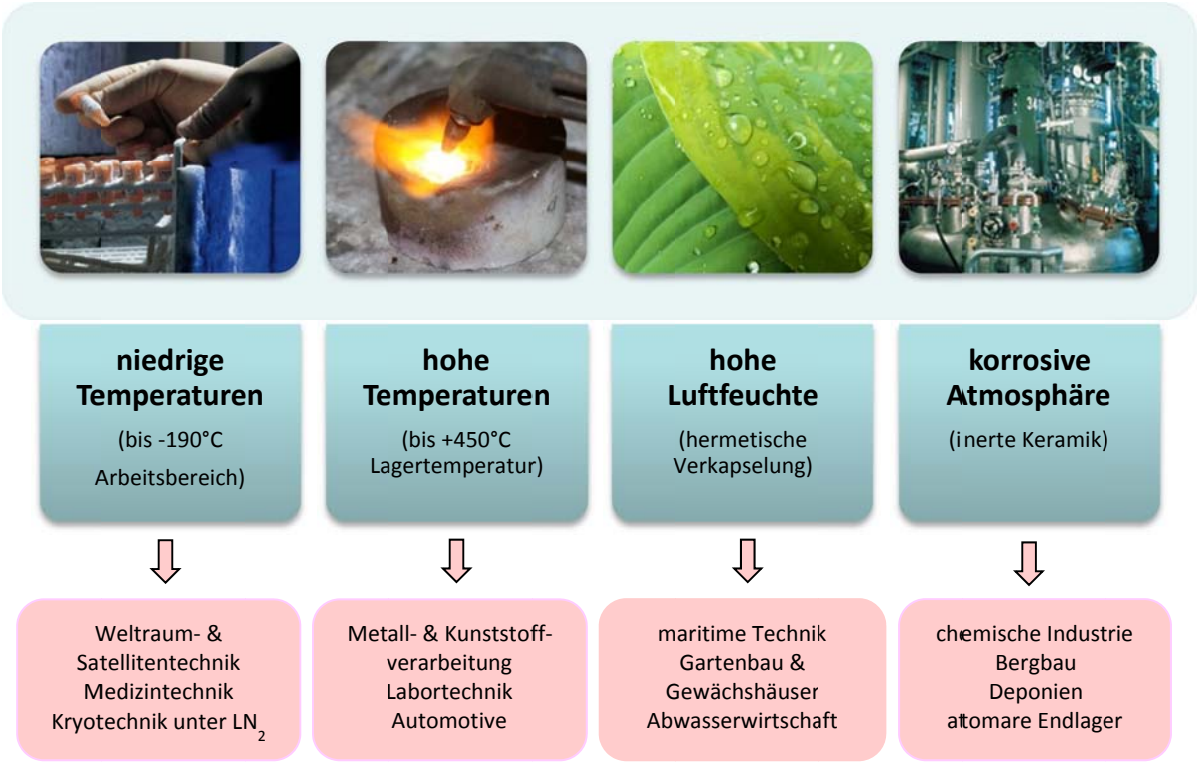


Abb. 32) Einsatzgebiete der XTC-ID Technologie

Basierend auf unserem Patent[3)] werden zunächst die, bei herkömmlichen Transpondern üblichen kunststoffhaltigen Trägermaterialien, gegen keramische Substrate ersetzt. Als keramische Materialien sind insbesondere Verbindungen aus Nitriden oder Oxiden vorgesehen. Der Chip sowie die Antennenstruktur können dabei entweder direkt in Keramik eingebettet, oder oberflächlich in SMD (Surface-Mounted-Design) Technik assembliert werden. Die elektrisch leitfähigen Strukturen und Kontaktflächen sind von ihrer Materialzusammensetzung her, dem keramischen Substrat

angepasst. Insbesondere physikalische Parameter, wie z.B. aufeinander abgestimmte Wärme-ausdehnungskoeffizienten sind entsprechend zu berücksichtigen. Neben metallischen Legierungen wie Au/Pd (Gold/Palladium) oder Ag (Silber) nano-Partikel, die typischerweise für diese Art von Leiterbahnen benutzt werden, gibt es aber auch Nichtmetalle, die eine elektrische Leitfähigkeit aufweisen und dabei den keramischen Materialien, beispielsweise in Bezug auf thermische Ausdehnungskoeffizienten noch ähnlicher sind.

Gerade das chemische Element Kohlenstoff erlebt seit einigen Jahrzehnten eine Renaissance in der Materialwissenschaft. Angefangen von Kohlenstofffasern, über Kohlenstoff nano-Röhrchen (Carbon nano-Tubes) bis hin zu den eindimensionalen Graphen-Schichten. Interessanterweise bilden Bornitrid (hBN) und Graphit ein isoelektronisches Paar zueinander, d.h. neben einer identischen Gitterstruktur (hexagonales Schichtengitter) sind auch viele der physikalischen Eigenschaften ähnlich ausgeprägt. Unterschiede gibt es nur in Farbe und elektrischer Leitfähigkeit. So ist Bornitrid eine farblose bzw. weiße nichtleitende Verbindung, während das schwarze Graphit eine gute elektrische Leitfähigkeit besitzt. Die Kombination von Bornitrid als keramisches Trägersubstrat und Graphit als Leiterbahn Material, wäre demnach eine denkbare Materialauswahl für den Einsatz bei hohen Temperaturen.

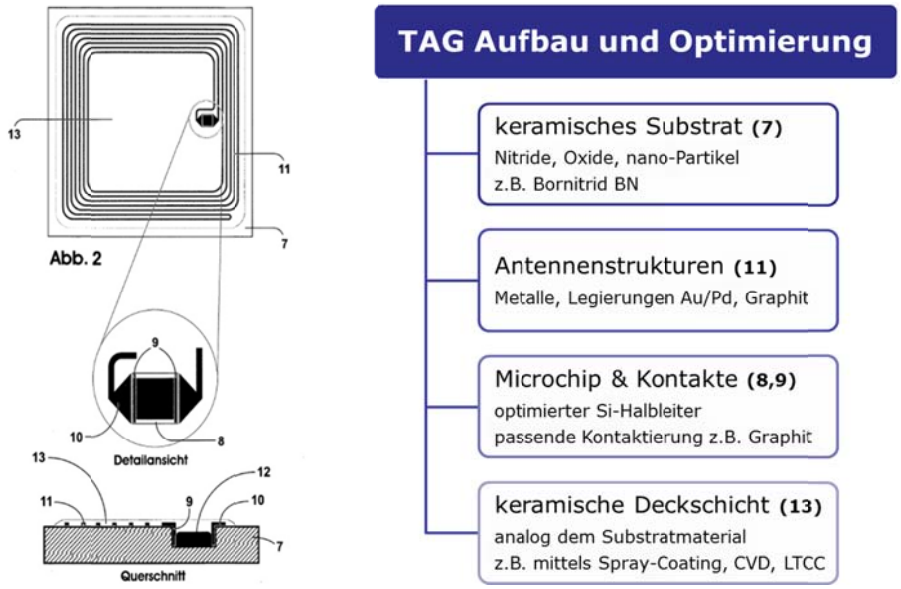


Abb. 33) XTC-ID TAG Aufbau & Optimierung

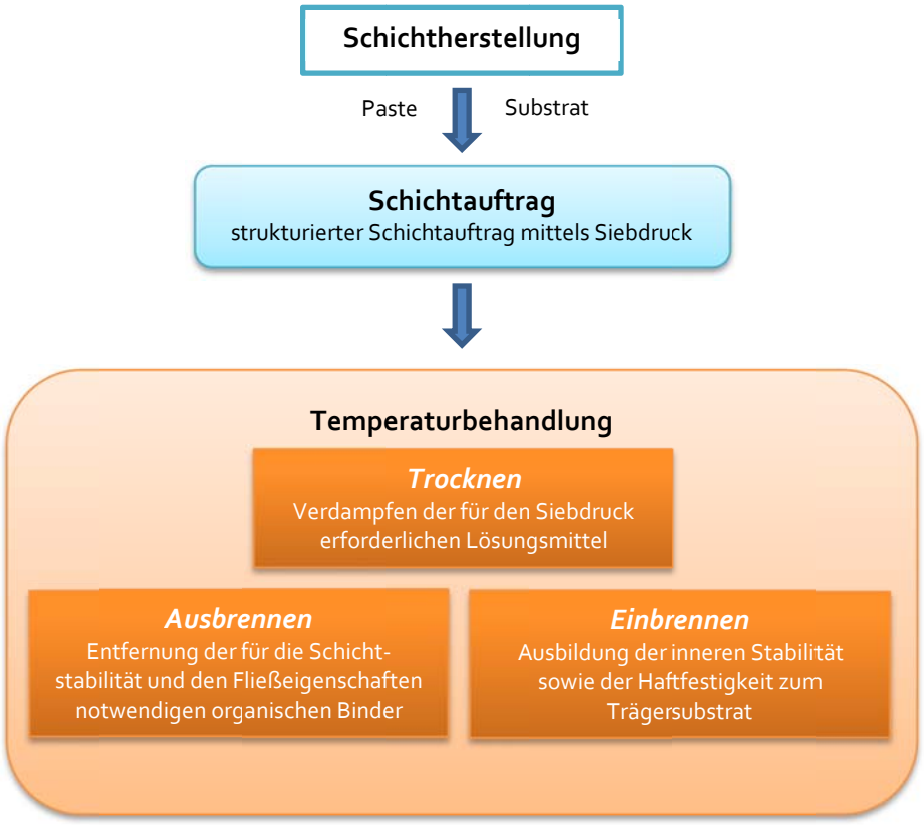
Durch Optimierung der Materialzusammensetzung (Abb. 33) gilt es letztendlich, den thermischen und mechanischen Stress, vornehmlich bei extremen Temperaturen zu verringern. Ergebnisse dazu sind den folgenden Kapiteln zu entnehmen.

Obwohl der XTC-ID TAG mit RFID-Chips aller drei möglichen Basistechnologien (Tab 1) bestückt werden kann, wurden im Rahmen des Projektes die entsprechenden HF-Typen favorisiert. Diese besitzen aktuell die größte Marktdurchdringung und ermöglichen Anwendungen ohne zusätzliche Hardwareausstattung (neben einem NFC-fähigen Smartphone).

3.2 Keramische Trägersubstrate

Ausgangsstoffe für technische Keramiken sind anorganische, nichtmetallische und gleichzeitig in Wasser schwerlöslich Verbindungen, die nach dem „Brennen“ oder genauer dem Sinterprozess (bei Temperaturen von typischerweise +800°C) eine kristalline Struktur von mindestens 30% aufweisen. Sie zeichnen sich durch eine harte, zähe bis spröde und verschleißfeste Oberfläche aus, die aber andererseits eine nachfolgende mechanische Bearbeitung oder Formgebung stark einschränkt. Für den technischen Einsatz werden am häufigsten Verbindungen aus Oxiden und Nitriden, mit Elementen der 3. Hauptgruppe (Bor & Aluminium) des Periodensystems verwendet. Insbesondere Aluminiumoxid Keramik (Al_2O_3) wird in großen Mengen hergestellt und ist deswegen oft preisgünstiger als andere Keramiken. Durch Zusätze anderer Oxide vor dem Sintern, lassen sich zudem Mischoxide mit teiladaptierten Eigenschaften produzieren.

Bei der Auswahl eines geeigneten keramischen Materials für den XTC-ID TAG, kamen deshalb in den Vorversuchen zunächst 1 mm dünne Aluminiumoxid Plättchen zum Einsatz. Durch eine Dickschichtechnik wurden im ersten Schritt, die elektrisch leitfähigen Antennenstrukturen samt Kontaktflächen mit Au/Pd Standardpasten im Siebdruckverfahren ausgebildet und anschließend ausgebrannt.



Um den inneren Anschluss der Antennenspule elektrisch isolierend zum Chip zurückzuführen, musste vor dem Einbrennen, zunächst eine Isolationsbrücke aufgebracht und darauf mittels Siebdruck eine weitere Leiterbahn hergestellt werden. Nach dem Einbrennen erfolgte im letzten Schritt die

Chipkontaktierung gefolgt von dessen Verkapselung mit Keramikpaste. Einen funktionstüchtigen Prototyp nach obigen Verfahren zeigt Abbildung 34. Trotz zufriedenstellender Ergebnisse in ersten Temperaturstresstests, erwies sich die Verwendung fertig gebrannter Keramiksubstratplättchen als zu unflexibel, um beispielsweise den Chip in eine Vertiefung (Cavity) einzulagern. Deshalb wurde im weiteren Verlauf eine Dünnschichttechnik, basierend auf mehrlagige LTCC Folien für alle weiteren Herstellungsprozesse favorisiert.

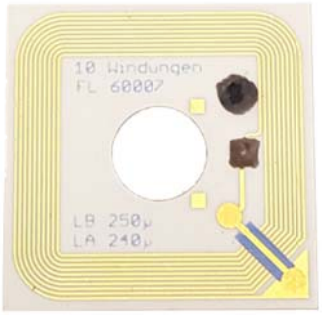


Abb. 34) TAG Prototyp nach Dickschichttechnik auf Al_2O_3-Substrat

3.2.1 LTCC-Technik & Materialauswahl

LTCC (low temperature co-fired ceramic) steht für ein Keramiksubstratsystem, das in der Elektrotechnik als preiswerte Substrattechnologie eingesetzt wird, wobei nahezu beliebig viele Lagen übereinander gestapelt werden können. Als Leiterbahnmetallisierung kommen üblicherweise Gold oder Silber bzw. deren Legierungen mit Platin und Palladium zum Einsatz. Die Metallisierungen werden im Siebdruckverfahren Lage für Lage auf die ungebrannte Keramik gedruckt und später, nach dem Stapeln und Pressen des vielschichtigen Aufbaus gemeinsam im Prozessofen gebrannt. Diese Technik wird als co-firing bezeichnet und gibt LTCC seinen Namen. „Low Temperature“ bedeutet in diesem Fall, dass die Sintertemperatur der Glaskeramik unter 900°C liegt. Diese relativ niedrige Temperatur ermöglicht erst den Einsatz von Gold- und Silberleiterbahnen, deren Schmelzpunkte zwischen 960°C und 1100°C liegen. Die Materialsysteme mit geringen dielektrischen und ohmschen Verlusten eignen sich gut für die Integration von Mikro- und Millimeterwellenschaltungen.

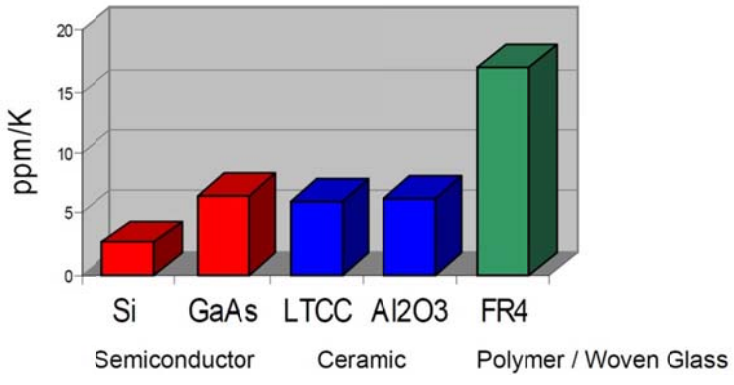


Abb. 35) Thermischer Ausdehnungskoeffizient verschiedener Substratmaterialien

Auch beim Vergleich der thermischen Ausdehnungskoeffizienten zwischen LTCC und Si-Halbleitern ergeben sich zumindest ähnliche Werte. Für den Einsatz im XTC-ID TAG wären zwar Galliumarsenid (GaAs) Halbleiter noch besser geeignet (Abb. 35), diese sind zurzeit in Form von RFID-ICs noch nicht verfügbar. Der LTCC-Prozess hat sich überall dort bewährt, wo hohe Anforderungen an die Zuverlässigkeit, insbesondere auch an die mechanische und klimatische Belastbarkeit, gestellt werden. Das sind zum Beispiel Anwendungen im Automotivbereich, in der Medizin, in der Sicherheitstechnik und in der Luft- und Raumfahrt. Die Verfügbarkeit von verlustarmen und hochfrequenzgeeigneten Materialsystemen (bestehend aus LTCC Grünfolien, abgestimmten Siebdruckpasten für Leiterbahnen, Durchkontaktierungen sowie speziellen Widerständen und Kondensatoren) in Kombination mit einer verbesserten Fertigungstechnologie, erweitern den Anwendungsbereich für LTCC-Applikationen bis hinauf zu Millimeterwellenfrequenzen (≤ 250 GHz).

Ein wesentlicher Vorteil der LTCC-Technologie ist dabei die Möglichkeit, passive Komponenten auch in Innenlagen zu integrieren ("vergrabene Bauteile"). So können Anpassnetzwerke, Koppelstrukturen und Filter im Innern des Mehrlagenaufbaus realisiert werden, welches die Integrationsdichte weiter erhöht. Auf diese Weise wird in den Außenlagen mehr Platz für ungehäuste Bauteile und SMT-Komponenten (oberflächenmontierte Bauteile) geschaffen. Die dreidimensionale Aufbau- und Verbindungstechnik der LTCC-Substrate umfasst neben den oben erwähnten passiven Komponenten (Kondensatoren, Widerstände und Spulen) auch planare Wellenleiter wie Mikrostreifenleiter, Koplanarleitungen in der Außenlage und geschirmte Streifenleiter in den Innenlagen. Dazu gehören auch Impedanz kontrollierte und geschirmte Übergänge zwischen den Ebenen des Mehrlagenaufbaus. Substratgefüllte Hohlleiter (SIW) stellen, vor allem im Frequenzbereich zwischen 30 und 80 GHz, eine interessante, weil verlustarme Alternative zu den Streifenleitern dar. Damit sind neue Lösungen möglich, die in herkömmlichen planaren Aufbau- und Verbindungstechniken wie Dickschichttechnik, Dünnfilmtechnik oder Halbleiterintegration (MMIC) nicht realisierbar sind. Diese komplexen Aufbauten müssen vor allem bei Millimeterwellenanwendungen sehr genau und reproduzierbar gefertigt werden (Abb. 36).

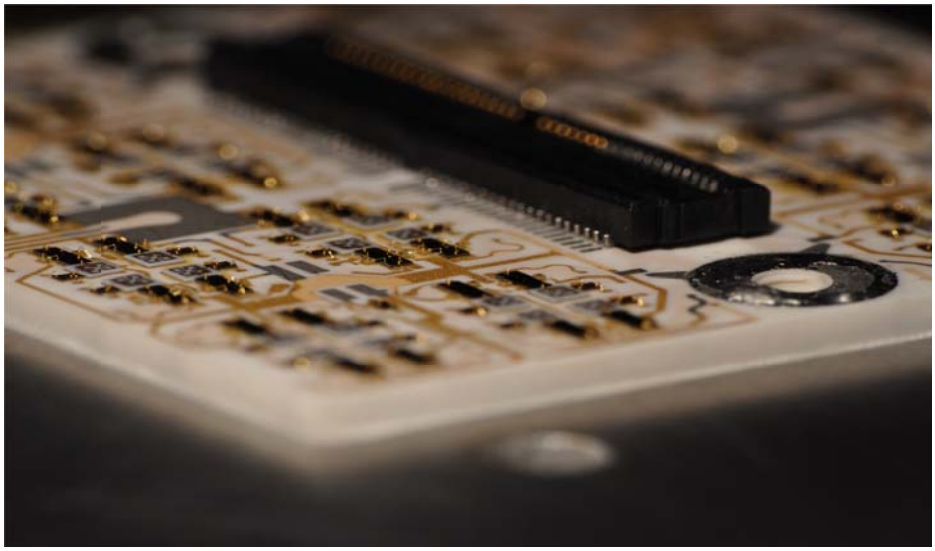


Abb. 36) SANTANA Antennenmodul, zirkular polarisiertes Antennenarray mit 8 x 8 Elementen[5)]

Besonders interessant ist das ungebrannte LTCC Material in Form der sogenannten „Grünfolien“. Einfach ausgedrückt handelt es sich hierbei um eine dünne Kunststofffolie (Schichtdicke < 250 µm), vergleichbar mit einer herkömmlichen Laminier- oder PVC-Folie, in der hohe Gewichtsanteile an nano-Partikel eines keramischen Materials (z.B. Aluminiumoxid) eingebettet sind. Das Polymer dient in diesem Fall nur als Stützstruktur während der Formvergebung. Im Gegensatz zum gebrannten Endprodukt, lässt sich die Folie beliebig falten oder biegen und mit simplen Werkzeugen wie einer Schere bearbeiten. Ebenfalls kann die Folie in diesem Zustand mit geeigneten leitfähigen Pasten oder auch anorganischen Farbpigmenten (z.B. Kobalt(II)oxid, CoO) bedruckt werden. Ebenso ist es möglich mehrere Folie aufeinander zu stapeln, um zum einen die Schichtdicke und damit die Stabilität zu erhöhen und zum anderen eine flexible elektronische Funktionalität zu ermöglichen. Ein analoger Ansatz wird übrigens bei anderen adaptiven Fertigmethoden, wie beispielsweise dem 3D-Druck von keramischen Materialien verfolgt. In diesem Fall werden die entsprechenden nano-Partikel direkt in das PA-Filament (Polyamid) eingebracht. Der komplette Arbeitsablauf zur Produktion eines LTCC-Substrats für einen XTC-ID TAG mit eingebetteter Antenne und Chip ist in Abbildung 37 beispielhaft dargestellt.

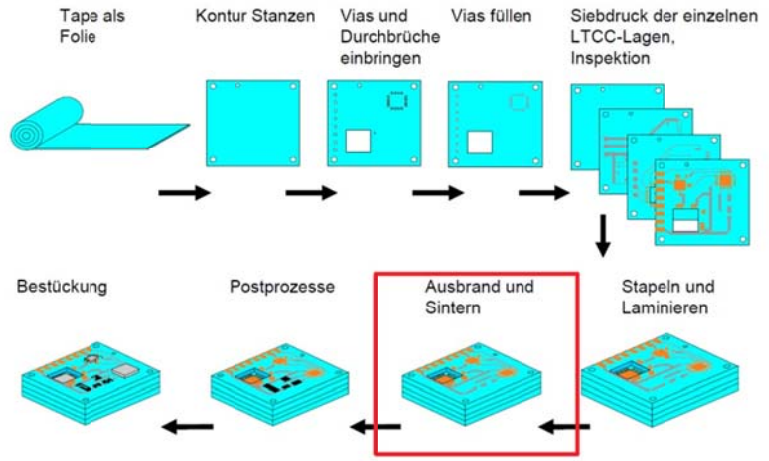


Abb. 37) Arbeitsschritte bei der LTCC-Fertigung[6)]

Um aus solchen weichen, formbaren Grünkörpern letztendlich harte Keramiken herzustellen, bedarf es jedoch einer erhöhten Aufmerksamkeit während des Brennvorgangs. Unter Einhaltung der chemisch/physikalischen Materialparameter gilt es ein entsprechend angepasstes Temperaturprofil einzuhalten (Abb. 38). Vereinfacht lässt sich das Verfahren in zwei Abschnitte unterteilen. Im ersten Schritt geht es darum die polymere Stützstruktur schonend zu entfernen, ohne dabei die Stabilität des Systems zu beinträchtigen. Eine langsame Aufheizrate bis zum ersten Haltepunkt bei 400°C ermöglicht hier das Ausgasen von Wasserdampf (Luftfeuchtigkeit) und anderer leicht flüchtiger Verbindungen. Ab Temperaturen von 350°C bis 550°C beginnen die organischen Binder und Weichmacher zu oxidieren bzw. zu verbrennen. Um gasförmige Zerfallsprodukte (CO, CO_2 usw.) zu erhalten, sollte demnach der gesamte Brennvorgang unter Luft bzw. Sauerstoffatmosphäre stattfinden. Je nach Anzahl an Folienlagen wird die Haltezeit entsprechend verlängert, um das Ausbrennen auch in inneren Schichten vollständig abzuschließen. Anschließend beginnt die eigentliche Pyrolysephase bis zu Temperaturen nahe dem Glaspunkt der keramischen Füllstoffe

zwischen 650°C bis 825°C. Alle restlichen organischen Verbindungen werden hierbei verascht und entweichen als gasförmige Zersetzungsprodukte. Am Glaspunkt findet ein Erweichen der anorganischen Stoffe in einem zähen amorphen Zustand statt. Dieser stellt gleichzeitig den Beginn der Sinterphase dar (Marker 4, Abb. 38).

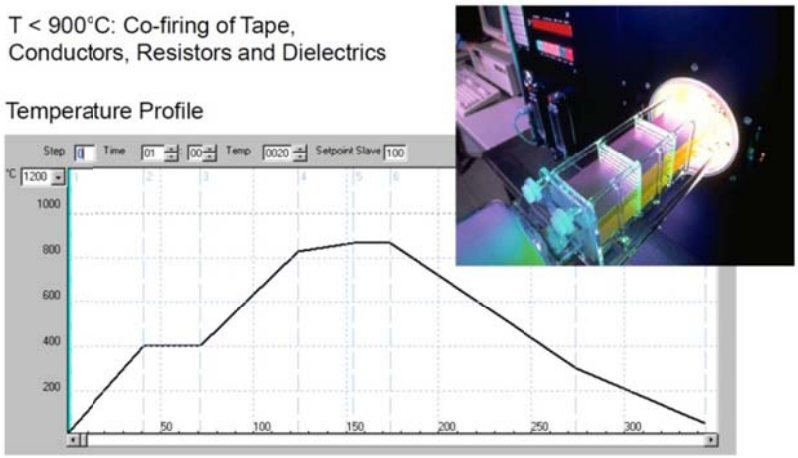


Abb. 38) Temperaturprofil zum Brennen von LTCC-Tape[5)]

Die entsprechende Haltezeit muss so bemessen werden, dass für den langsam fließenden Glasanteil der Keramik ebenfalls der Sinterprozess abgeschlossen wurde (Einbrennphase). Anschließend erfolgt eine ballistische Abkühlkurve auf Raumtemperatur, um thermische Spannungen innerhalb des Substrats während des Rekristallisationsprozesses zu verhindern. Wichtig anzumerken ist, dass jeder Sintervorgang zu einem Schrumpfprozess führt, d.h. der Grünkörper muss um einen Faktor überdimensioniert werden, damit die eigentliche Zielgröße erreicht wird. Im Fall der LTCC-Materialien ist dieser Schrumpfprozess gleichmäßig und reproduzierbar, fällt aber je nach Typ unterschiedlich aus (Abb. 39).

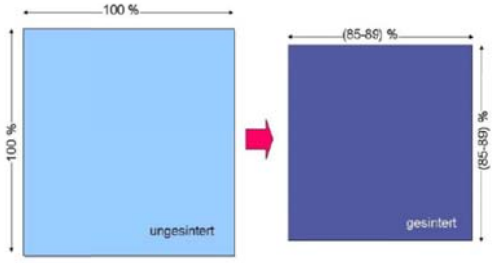


Abb. 39) Sinterschrumpf Effekt bei LTCC-Materialien[7)]

Im Fall des XTC-ID TAGs muss insbesondere die Ausbrennphase vollständig abgeschlossen sein. Eventuelle Rückstände an organischen Verbindungen, würden bei einer erneuten thermischen Belastung ansonsten als Gase aus den inneren Schichten entweichen und zu Rissen im Substrat und damit zu einem Totalausfall führen. Zudem müssen toxische Belastungen während der gesamten Einsatzzeit hinweg auszuschließen sein. Zur Überprüfung des Brennvorgangs eignen sich besonders chemische Analysemethoden (wie Pyrolyse/GC/MS) an fertigen „co-fired“ Materialproben gleicher Schichtdicke, jeweils mit und ohne Metallisierung.

3.2.2 Chemische Materialuntersuchungen

Alle Materialanalysen wurden an einem Agilent 7890B GC/5977B MSD System, mit CDS Pyroprobe 6200 zur Probenaufgabe durchgeführt. Dazu wurden kleine Probenstücke des fertig ausgebrannten LTCC-Substrats in Quarzröhren überführt und im Pyrolysator sowohl unter Helium- als auch Normalluft Atmosphäre mittels eines Temperaturprogramms erhitzt. Die Maximaltemperatur betrug zunächst +450°C bei einer Pyrolysezeit von 15 Sekunden und entsprach so der geplanten Einsatztemperatur eines XTC-ID TAGs. Die Empfindlichkeit dieser Analysenmethode ist anhand der beiden unteren Chromatogramme aus Abbildung 40 deutlich zu erkennen. So wurden die Proben am Anfang der Untersuchungsreihen zunächst in Plastikbeuteln verpackt gelagert. Diejenigen Proben, die dabei direkten Kontakt mit der Kunststoffoberfläche hatten, zeigten im ersten Durchlauf einen signifikanten Weichmacher (Phthalsäureester) Peak bei 16,5 Minuten, während Proben aus Mittellagen keinerlei Verunreinigungen zeigten (rote Kurve).

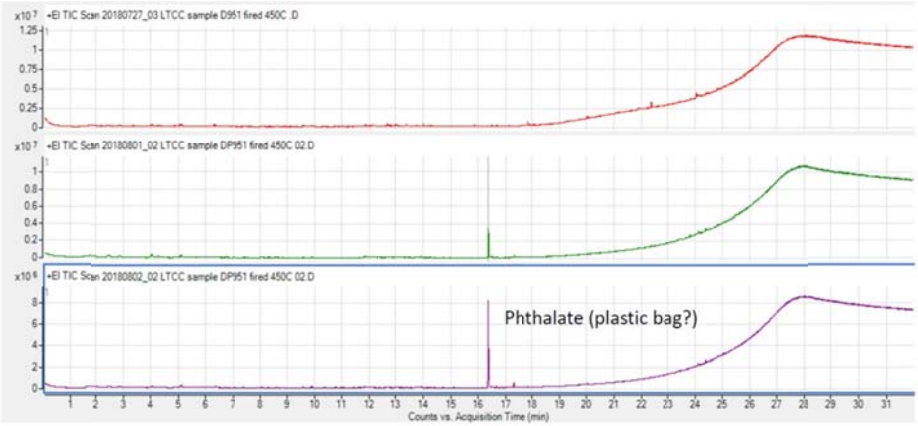


Abb. 40) py-GC-MS Chromatogramm (Emissionsprofile, volle Heizrate auf 450°C, 15 s, Helium)

Um solche Kontaminationen im weiteren Verlauf auszuschließen, wurden neue Probenkörper in Standarddimension (1×1×1 mm) für nachfolgende Untersuchungen extra angefertigt und in Glasvials gelagert. Dadurch konnten Verunreinigungen ausgeschlossen und die Reproduzierbarkeit der Messungen deutlich erhöht werden. Insgesamt wurden drei unterschiedliche LTCC-Materialien verschiedener Hersteller überprüft (Tab. 3).

#	LTCC-Materialtyp	Metallisierung
1	FERRO A6M-E	ohne
2	FERRO A6M	ohne
3	FERRO A6M	Gold (Au)
4	DuPont 951	Silber (Ag)
5	DuPont 951	Gold (Au)
6	DuPont 9k7	Gold (Au)
7	DuPont 9k7	Gold (Au), Silber (Ag), Platin (Pt), Palladium (Pd)

Tab. 3) Liste der untersuchten LTCC-Materialien

Interessant wäre es natürlich vorab, die anorganischen & organischen Bestandteile einzelner LTCC-Materialien zu kennen, damit eine Analytik entsprechend abgestimmt werden kann. Bezüglich der genauen Zusammensetzung geben die Datenblätter samt Sicherheitsanhängen der Hersteller, aber nur in begrenztem Maße Aufschluss. Nach eingehender Literaturrecherche fanden sich dennoch einige Quellen[8,9)], die zumindest Informationen über die anorganische Zusammensetzung lieferten. Die blaue Färbung der DuPont Materialien ergibt sich durch geringe Beimengungen von Kobaltoxid (CoO), welches in den Analysen der Tabelle 4 nicht berücksichtigt wurde. Die drei anorganischen Hauptkomponenten wurden jeweils in Fettschrift hervorgehoben. Der Einsatz von Mischoxiden im LTCC-Tape führt zu der gewünschten Schmelzpunkterniedrigung (kolligative Eigenschaften der Materie) im Sinterprozess, bei Temperaturen unter 900°C. Einkomponenten Material, beispielsweise aus reinem Aluminiumoxid, würde dagegen Sintertemperaturen von bis zu 2072°C benötigen. Unter dem Glühverlust fallen weiterhin alle organischen Verbindungen wie Binder und Weichmacher usw. die durch den Sinterprozess pyrolysiert und ausgetrieben wurden. Ihr Anteil liegt im Mittel bei 10% der Gesamtmasse. Auffällig ist, dass die DuPont Grünfolien als Hauptbestandteil ~50% Aluminium-oxid enthalten, während die anderen Folien vornehmlich auf Silikatbasis ($CaSiO_3$-Ferro bzw. $BaAl_2Si_2O_8$-Heraeus) aufgebaut sind.

Element	FERRO A6M	DuPont 951 AX	Heraeus CT 700	DuPont 943 HF
Glühverlust (organische Substanzen)	12,58	11,63	8,21	10,23
SiO_2	**37,06** (48)	**27,20** (47)	**32,86** (42)	0,36 (4)
CaO	**31,54** (47)	4,03	3,15	6,84
MgO	0,13	0,35	2,97	0,03
B_2O_3	**15,09**	1,75	0,48	**15,93**
Al_2O_3	0,13	**42,43** (42)	**19,62** (31)	**49,45** (76)
PbO	<NWG	**8,25**	0,68	0,04
ZnO	<0,01	0,02	4,50	---
SrO	<0,01	<NWG	4,95	---
BaO	<NWG	<NWG	**16,01** (5)	---
La_2O_3	---	---	---	**15,75**

Tab. 4) Chemische Zusammensetzung der LTCC Grünfolien[8)] & blau markiert[9)] (<NWG = unterhalb der Nachweisgrenze)

Drastisch sind dagegen die Unterschiede in der prozentualen Massenverteilung der Haupt-komponenten, im direkten Vergleich beider Literaturstellen (blau gekennzeichnete Werte in Tab 4) zu bewerten. Zudem werden in Literaturquelle[9)] die Elemente Kalium (K), Titan (Ti) und Kobalt (Co) nachgewiesen, während Blei (Pb), Bor (B), Strontium (Sr) sowie Lanthan (La) nach Quelle[8)] fehlen. Hier wurde als Analysenmethode die Energiedispersive Röntgenspektroskopie[9)] (EDX/EDS) gewählt, während die genaue Messmethodik im anderen Fall nicht beschrieben wurde. Derart starke Abweichungen sind aber eher auf systematische Fehler zurückzuführen, als auf unterschiedliche Messverfahren. Da zudem die Werte bei allen untersuchten Typen und Herstellern abweichen, sind externe Ursachen unwahrscheinlich. Die Daten aus Tabelle 4 sind demnach mit Vorsicht zu behandeln.

Die organischen Binder und Weichmacher kommen in Form zweier unterschiedlicher Polymere-Systemen zum Einsatz. Sie werden als temporäre Bindemittel für LTCC-Folien verwendet, da sie bei Temperaturen oberhalb 400°C rückstandsfrei verbrennen. Die Heraeus Materialien sollen als Basis Polyvinylbutyral (PVB) benutzen[9)]. Dabei handelt es sich um einen Kunststoff aus der Gruppe der Polyvinylacetale, der technisch unter anderem auch als Zwischenschicht in Verbundgläsern Anwendung findet. Die beiden anderen Hersteller DuPont und Ferro verwenden, ebenfalls laut Literaturstelle[9)], Acrylate bzw. Acrylharze (Polymere der Acrylsäureester) als keramischen Binder. Ein Blick in das Sicherheitsdatenblatt der Ferro A6M Folie (Abb. 41) zeigt dagegen eine falsche Zuordnung auf. Auch diese Folie verwendet Polyvinylbutyral als Polymere Matrix der organischen Komponente, während der anorganische Anteil aus einem Bor-Silikat-Glass Mischoxid besteht und demzufolge genau der Zusammensetzung der Tabelle 4 entspricht.

1. Stoff-/Zubereitungsbezeichnung

SD-Blatt	: 22976
Lieferant	: FERRO ELECTRONIC MATERIAL SYSTEMS VISTA 1395 aspen way 92083 vista California Vereinigten Staaten von Amerika Tel: 760-305-1000 Fax: 760-305-1100
Handelsname	: A6-M TAPE
Allgemeine Umschreibung	: .
Anwendung	: Divers
Publikationsdatum	: 2005-11-29
Allgemeine information	: dangerous.goods@philips.com
Notruf Telefonnummer	: +31 (0)497-598315

2. Zusammensetzung/Angaben zu den Bestandteilen

Bestandteil	CAS-nr	EG-nr	Katalog-nr	Prozentsatz(%)
OXYDIPROPYLBENZOAT	27138-31-4	248-258-5		≥1.0 - <5.0
BORON SILICATE GLASS POWDER	65997-17-3	266-046-0		≥50.0 - <80.0
POLYVINYL BUTYRAL POLYMER	27360-07-2			<15.0
BENZYL BUTYL PHTHALATE	85-68-7	201-622-7	607-430-00-3	<1.0
BIS(2-ETHYLHEXYL)PHTHALAT	117-81-7	204-211-0	607-317-00-9	<1.0
TOLUOL	108-88-3	203-625-9	601-021-00-3	<1.0

Abb. 41) Ferro A6M Sicherheitsdatenblatt (Auszug)

Nach diesem Streifzug durch die Literatur, erfordern die weiteren massenspektroskopischen Untersuchungen, eine Erhöhung der Nachweisgrenze durch Anreichung der flüchtigen Stoffe auf einem Adsorbens (Tenax-Trap), um überhaupt die Chance zu bekommen, Reste der rückstandslos verbrennenden Komponenten zu detektieren. Praktisch sieht die Vorgehensweise so aus, dass jeweils fünf frische Proben, bei einer verlängerten Pyrolysezeit von fünf Minuten (vorher 15 Sekunden), hintereinander pyrolysiert und die austretenden flüchtigen Bestandteile auf einer gekühlten Adsorbensfalle angereichert werden. Anders ausgedrückt, werden die gasförmigen Verbindungen der ersten vier Zyklen auf der Falle zwischengeparkt und so angereichert. Erst nach der fünften Probe wird die Adsorbensfalle aufgeheizt, um die gesammelten Eluenten gleichzeitig auszutreiben und einer GC/MS Analyse zuzuführen. Anstatt einer Probe entspricht, dass Konzentrationsverhältnis somit dem einer fünffachen Probenmasse. Die ebenfalls denkbare, wiederholte Pyrolyse einer einzelnen Probe mit Anreicherung, führt dagegen nicht zum Ziel. Schon nach der ersten Temperaturbehandlung ließen sich bei allen Proben keine flüchtigen Verbindungen mehr nachweisen (Abb. 42). Dies ist in Übereinstimmung mit Untersuchungen[10)] für den Einsatz von Bauteilen aus LTCC-Materialien in Massenspektrometern mit Ionenfallen (Ion Traps).

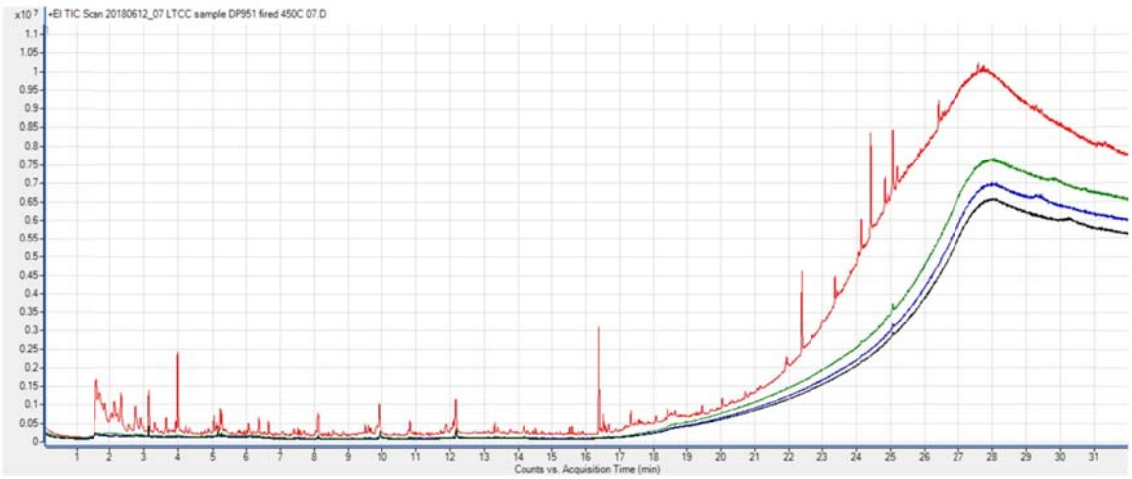


Abb. 42) Chromatogramme einer Probe nach wiederholtem Aufheizen (+450°C, 15 Sekunden)

Den Effekt zwischen einem direkten Pyrolyselauf (grünes Chromatogramm) und einer nach obigen Verfahren angereicherter Messung (rotes Chromatogramm) zeigt eindrucksvoll die Abbildung 43. Während im ersten Fall die Peaks im Signalrauschen der Basislinie „untergehen“, zeigen diejenigen des angereicherten Chromatogramm, eine um ca. zwei 10er Potenzen höhere Signalamplitude bei ausreichender Basislinientrennung.

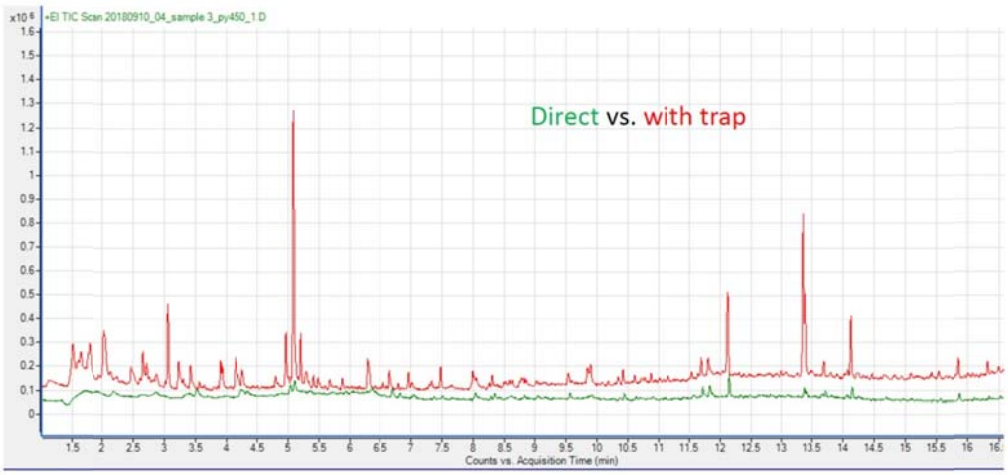


Abb. 43) Vergleich zwischen einmaligem (direkt) & angereichtem (trap) pyro-GC-MS Lauf

Das Adsorbensmaterial Tenax® (Poly(2,6-diphenyl-p-phenylenoxid) stellt gleichfalls ein polymeres Harz mit Beimengungen aus Chromosorb® (Styrol-Divinylbenzol) dar und ist nur bei Temperaturen bis 350°C temperaturstabil. Durch Blindläufe (blank runs) ist deshalb sicherzustellen, dass Verunreinigungen bzw. Zersetzungsprodukte aus dem Adsorbens entsprechend erfasst und markiert werden (Abb. 44). Darunter fallen insbesondere die beiden monomeren Zerfallsprodukte Styrol und Methylstyrol. Auf eine ebenfalls mögliche mathematische Subtraktion des Blindlaufs vom Probenlauf unter Glättung der Datenpunkte wurde verzichtet. Alle Chromatogramme zeigen reine Rohdaten.

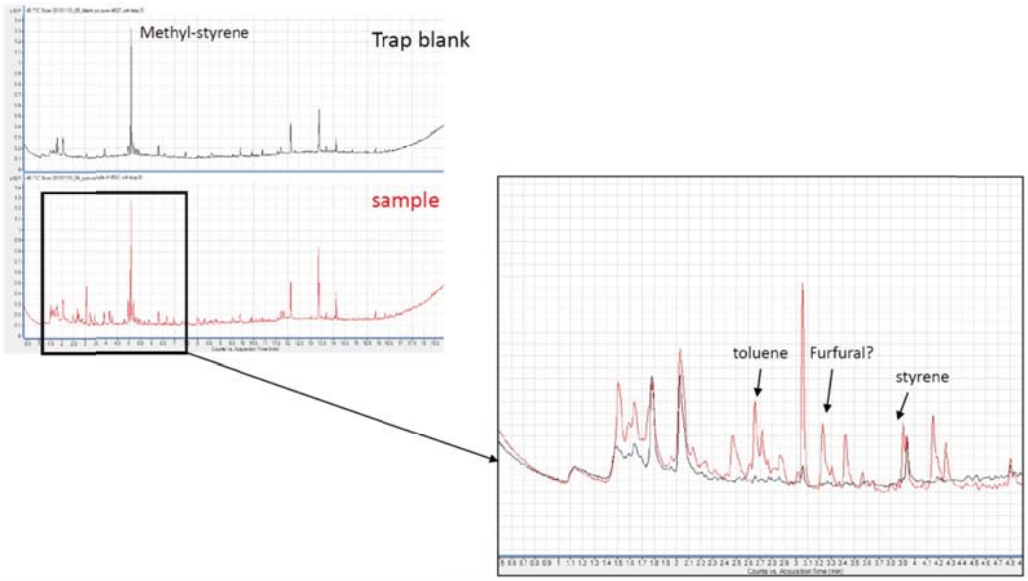


Abb. 44) Vergleich zwischen Blind- und Proben Chromatogramm (pyro-trap-GC-MS Lauf)

Der Vergleich zwischen Chromatogrammen bei einer Pyrolyse unter Inertgas (Helium) mit denen unter Luft, zeigen ebenfalls keine weiteren Peaks, beispielsweise von Zersetzungsprodukte durch Oxidationsprozesse (Abb. 45). Alle integrierbaren Peaks sind ebenso im Blindlauf enthalten und stammen vornehmlich vom Adsorbens- bzw. Trennsäulenmaterial.

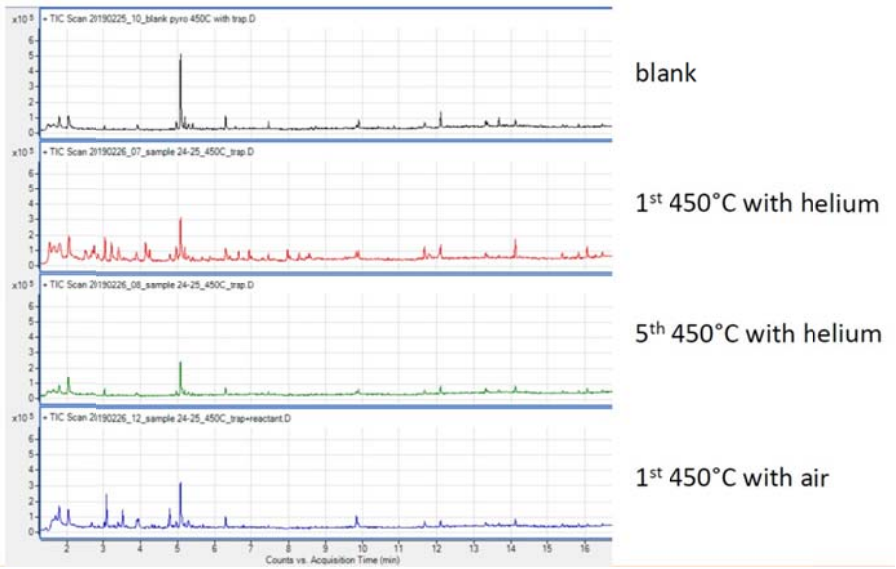


Abb. 45) Pyrolyse-Chromatogramme von LTCC-Materialien unter Helium & Luft Atmosphäre

Zusammenfassend lässt sich feststellen, dass anhand der chemischen Materialanalysen an „co-fired“ LTCC-Proben keinerlei flüchtige Verbindungen oder Schadstoffe nachweisbar waren. Das XTC-ID Substrat ist bis zu der geplanten Einsatztemperatur von +450°C, somit toxisch als vollkommen unkritisch zu bewerten. Weiterhin weisen die Ergebnisse darauf hin, dass der Ausbrennprozess nach dem gewählten Temperaturprofil vollständig abläuft und keine Rückstände verbleiben.

3.2.3 Physikalische Materialuntersuchungen

Anhand der Rasterelektronenmikroskopie (SEM-Scanning Electron Microscope) wurde an der UNI Twente zunächst die physikalische Struktur, der im XTC-ID Substrat verwendeten LTCC- Grünfolien untersucht. Daraus sind Rückschlüsse über Produktionsverfahren, Qualitätsstandards, Porosität bzw. Partikelverteilung und reproduzierbare Sinterprozesse zu gewinnen. Hier würde eine hohe Exemplar Streuung innerhalb einer LTCC-Tape Charge, im Umkehrschluss zu einer höheren Ausschussrate beim XTC-ID Substrat führen.

Um Aufladungseffekte bei der SEM-Untersuchung von elektrischen Isolatoren zu vermeiden, wurde das LTCC-Material während der Probenvorbereitung mit Graphit bedampft (Abb. 46), anschließend ein Materialquerschnitt entnommen und dieser der Hochvakuumkammer zugeführt.

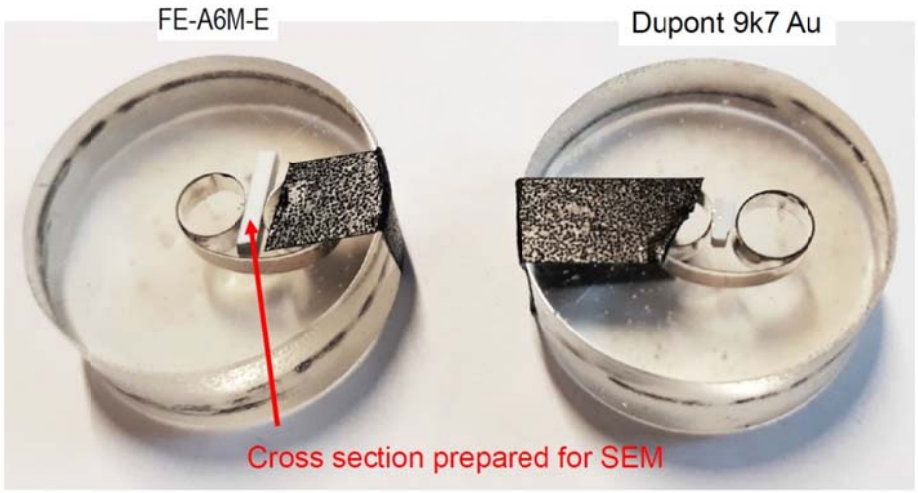


Abb. 46) Probenvorbereitung an LTCC-Grünfolien

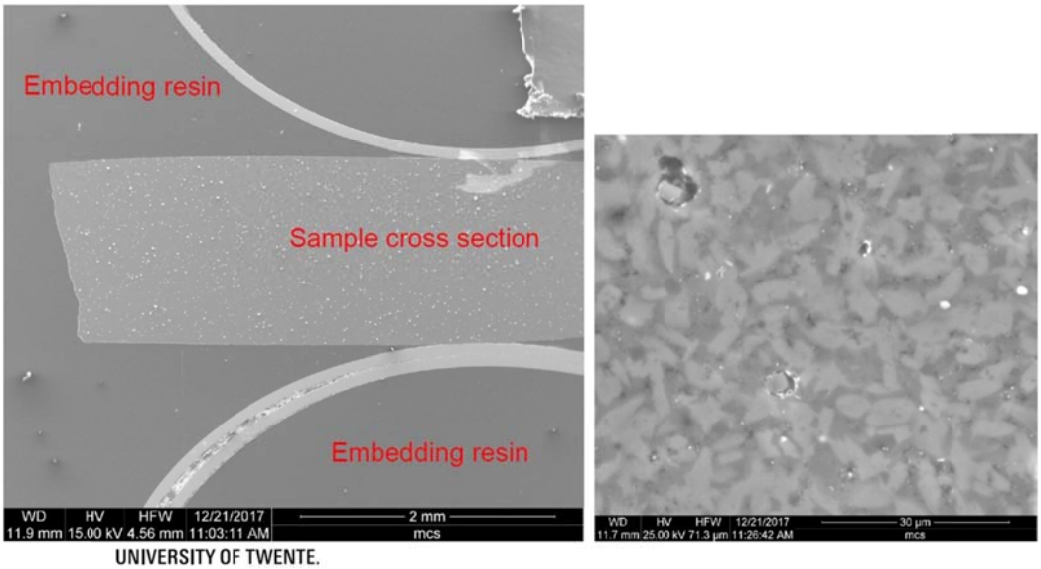


Abb. 47) SEM-Aufnahme der LTCC-Folie, Typ Ferro A6-M

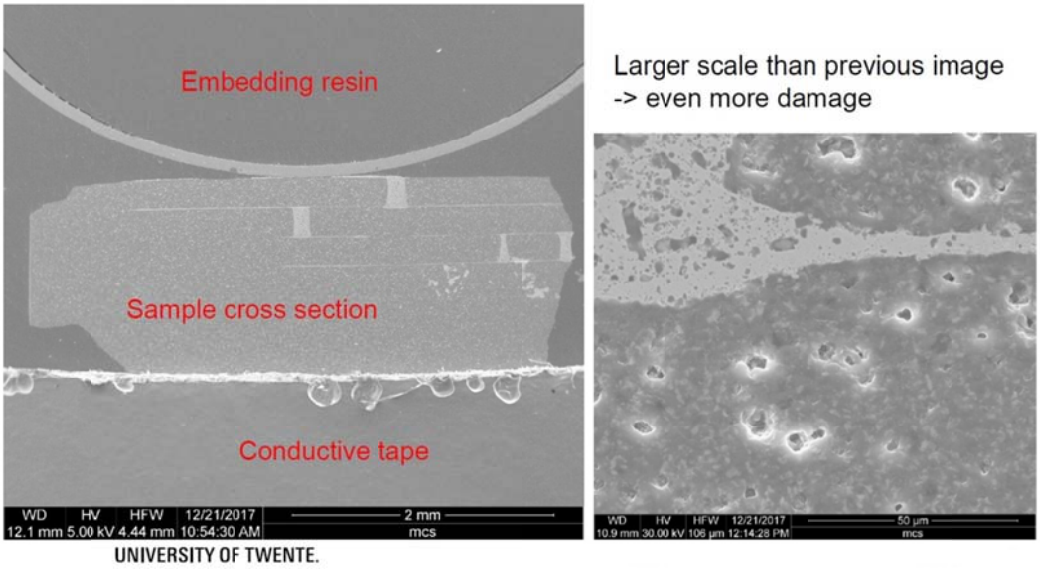


Abb. 48) SEM-Aufnahme der LTCC-Folie, Typ DuPont 9K7

Beide Aufnahmen zeigen die Morphologie der LTCC-Grünfolien. Während das Ferro A6-M Material (Abb. 47) aus größeren clusterförmigen Partikeln aufgebaut ist, scheinen diese im DuPont Material (Abb. 48) deutlich kleiner und gleichmäßiger verteilt zu sein. Auffällig sind jedoch Artefakte und Fehlstellen innerhalb beider Materialproben. Diese zeigen allerdings keinen Effekt auf die Substratqualität nach dem Sintern. Solange die Fehlstellen klein genug und genügend keramische Partikel vorhanden sind, fließen diese bei der Glastemperatur zusammen und bilden danach eine geschlossene Struktur. Alle XTC-ID Substrate wurden dabei nach dem Laminieren der vier Einzellagen (Abb. 37), ohne äußeren Druck und ohne Fixierung flach ausgelegt und unter Atmosphärendruck gebrannt. Bis auf einige Testmuster, wurde ausschließlich das DuPont 951 LTCC-Tape für den XTC-ID TAG verwendet, da es eine bessere Oberflächenbeschaffenheit (geringere Rauigkeit) sowie bessere elektromagnetische Eigenschaften im HF-Band aufwies (Tab. 5).

Material	Size [mm]	Layers	Turns	Simulated XL [Ohm] @ 13.56 MHz	Measured XL [Ohm] @ 13.56 MHz	Reading Distance [mm]
DuPont 951	10×10*	4	4x7	---	590	28
	10×10	4	4x7	490	560	33
	25×25	1	11	443	475	61
	33×33	1	9	514	590	69

*) engere Leiterbahnabstände der Antenne

Tab. 5) Simulierte und gemessene Spulenimpedanz & Lesereichweite der XTC-ID TAGs

3.3 Chiptypen Auswahl (HF-Band)

Eines der wichtigsten Komponenten im XTC-ID TAG stellt der Silizium-Chip als Halbleiterbauteil dar. Obwohl während der Projektvorbereitungsphase ebenfalls eine Halbleiterfertigung von neuartigen Galliumarsenid (GaAs) Prototypen in Betracht gezogen wurde, hätte eine solche Entwicklung den Projektrahmen gesprengt und wurde demzufolge zunächst verworfen. Stattdessen wurden in einem ersten Schritt, die kommerziell erhältlichen und dabei den XTC-ID Spezifikationen entsprechenden Typen evaluiert. Aufgrund der angestrebten hohen Temperaturbeständigkeit, kommen hier nur Halbleiterbauteile ohne eigene Verkapselung (Nacktchip oder „Bare Die“) in Betracht. Das weitere Anforderungsprofil erfordert:

- **geringe Chipdimensionen, bei gleichzeitig hoher Speicherkapazität (ca. 2 kBit)**
  Eine geringe Größe ist entscheidend um den Halbleiter später vollständig in Keramik verkapseln zu können und verringert thermische Belastungen im Siliziumgitter.

- **Chip direkt aus Wafer (Nacktchip/Bare Die), möglichst unbehandeltes Silizium**
  Keine Beschichtungen oder Verkapselungen, Chip Kontakte reines Metall (Au/Pd) ohne Lötpaste. Jede weitere Materialkomponente erschwert die Abstimmung („Matching“) der physikalischen Parameter.

- **Speichertechnologie als FRAM oder EEPROM**
  Neue FRAM (Ferro Electric Random Access Memory) Speicher zeigen sich robuster gegenüber den Bit-Flip Effekt einzelner Speicherzellen bei hohen Temperaturen oder unter Einwirkung von harter Gamma Strahlung. Sind aber, im Gegensatz zum EEPROM (Electrically Erasable Programmable Memory), aufgrund ihrer größeren Speicherzellen (geringere Speicherdichte) bislang kaum verfügbar.

- **HF-Chip mit NFC Kompatibilität nach ISO/IEC 15693**

Chip	ISO/IEC 15693	ISO/IEC 18000-3	ISO/IEC18000-63	ISO14443A	ISO14443B	NFC Forum Type 2	EPC Gen2 V2	Memory [bit] (Userdata)	Storage Temperature Tl [°C]	Storage Temperature Th [°C]	Operating Temperature Tl [°C]	Operating Temperature Th [°C]	Bare Die	Thickness	unsawn / Bumping	sawn / Bumping
EM4033	•	•						64	-55	125	-40	85	yes	6 mils	yes / no	yes / gold bump
EM4094	•			•	•				-50	150	-40	110	no	TSSOP 16 / SO20	-	-
EM4133	•							512	-55	125	-40	85	yes	11 mils	yes / no	yes / gold bump
EM4233	•							2k	-	-	-40	85	-	-	-	-
EM4233slic	•							1k	-55	125	-40	85	yes	6 mils	yes / gold bump	yes / gold bump
EM4237	•	•						2112	-55	125	-40	85	yes	3 mils / 6 mils / 29 mils	(29mils) yes / Standard aluminium pads	(3 /6 mils) yes / gold bump
EM4237slic/ slix	•	•						1k/2k	-55	125	-40	85	yes	3 mils / 6 mils / 29 mils	(29mils) yes / Standard aluminium pads	(3 /6 mils) yes / gold bump
EM4333	•			•							-40	85	-	-	-	-
EM4423			•	•		•	•		-50	125	-40	85	yes	6 mils	no	yes / gold bump

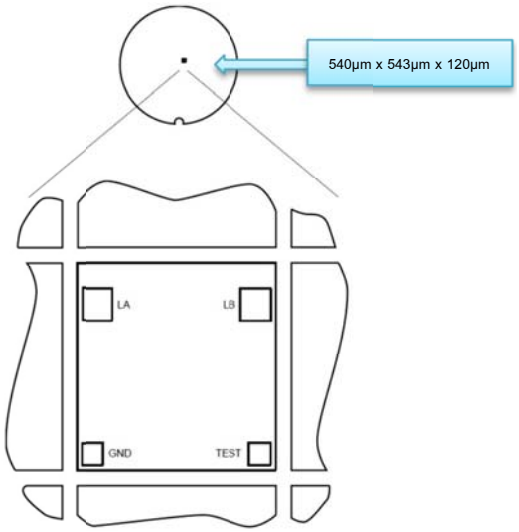
Tab. 6) Chip Typen im Vergleich (EM Microelectronic) *[3mils ≡ 76,2µm]*

Chip		ISO/IEC 15693	ISO/IEC 15693-3	ISO/IEC 18000-3	EPC Class 1 2	EPC Class-1 HF1	Memory [bit] (Userdata)	Storage Temperature Tl [°C]	Storage Temperature Th [°C]	Operating Temperature Tl [°C]	Operating Temperature Th [°C]	Bare Die	Thickness	unsawn / sawn / Bumping	unsawn / sawn / Bumping
SL2S2002	ICODE SLIX	•		•			896	-55	125	-40	85	yes	120 µm	no	yes / bumped
SL2S6002	ICODE DNA		•				2016	-55	125	-40	85	-	-	no	yes / bumped
SL2S2602	ICODE SLIX 2	•		•			2500	-55	125	-40	85	yes	120 µm	no	yes / bumped
SL2S5002	ICODE SLIX-L	•		•			256	-55	125	-40	85	yes	120 µm	no	yes / bumped
SL2S5302	ICODE SLIX-S	•		•	•		1280	-55	125	-40	85	yes	120 µm	no	yes / bumped
SL2S1402	ICODE ILT			•		•	-	-55	125	-40	85	yes	120 µm	no	yes / bumped
SL2S1412	ICODE ILT-M			•		•	512	-55	125	-40	85	yes	120 µm	no	yes / bumped

Tab. 7) Chip Typen im Vergleich (NXP Semiconductors) *[120µm ≡ 4,72mils]*

Die entsprechenden Recherche Ergebnisse (Stand März/2017) sind den Tabellen 6 und 7 zu entnehmen. Alle aufgeführten Hersteller geben dort Betriebstemperaturen von -40°C bis +85°C sowie Lagertemperaturen von -55°C bis +125°C für ihre Nacktchiptypen (Bare Die) an. Laut Herstellerangaben, lassen sich höhere Lagertemperaturen durch thermische Isolation erzielen, während auf tiefere Lagertemperaturen nicht explizit geprüft wurde. Alle recherchierten Typen basieren auf Silizium Halbleiterbasis und benutzen die EEPROM Speichertechnologie. Ergänzend soll eine Pressenachricht[11)] der Firma Fujitsu nicht unerwähnt bleiben, die erst zum Projektende veröffentlicht wurde. Hier wird über den Produktionsstart von Chips mit FRAM Speichertechnologie und einer Betriebstemperatur von +125°C berichtet. Durch die Übernahme von Cypress durch Infineon, sind nun ebenfalls FRAM Halbleiter mit erhöhter Betriebstemperatur von einem weiteren Hersteller verfügbar. Es ist davon auszugehen, dass diese Chiptechnologie zukünftig auch als RFID-Variante entwickelt wird und somit auch für den XTC-ID TAG ein interessantes Einsatzpotential liefern würde.

Für den Einsatz im XTC-ID TAG wurde der ICODE SLIX 2 (SL2S2602FUD/BG[1)]) von NXP ausgewählt. Dieser wird in Form eines gesägten monokristallinen Si-Wafer (Format 200mm ≡ 8inch), bestehend aus 94.823 Stück Nacktchips (Bare dies) auf Blue Tape geliefert (Abb. 49). Die Chip Dimensionen betragen 540µm×543µm (0.29322mm^2) bei einer Dicke von 120µm, womit dieser äußert klein ausfällt und sich damit ideal zur Integration in einem Substrat Hohlraum (Cavity) eignet. Auf der Oberseite wurde der Wafer zum Schutz der „geätzten" Strukturen (CMOS 0,14µm), mit einer 1,75µm dicken Silizium Nitrid (Si_3N_4) als Passivierungsschicht, vornehmlich gegenüber Luftfeuchtigkeit sowie gegen Diffusions- und Oxidationseffekten beschichtet. In den Datenblättern[1)] wird diese Schicht oft als PE-nitride bezeichnet, wobei PE nicht für die Abkürzung des Kunststoffs Polyethylen steht, sondern in diesem Kontext, dass Beschichtungsverfahren PE-CVD (Plasma Enhanced-Chemical Vapor Decomposition) bezeichnet. Diese Schicht ist voll kompatibel mit den keramischen Substraten und vom Material her damit als unkritisch zu bezeichnen.



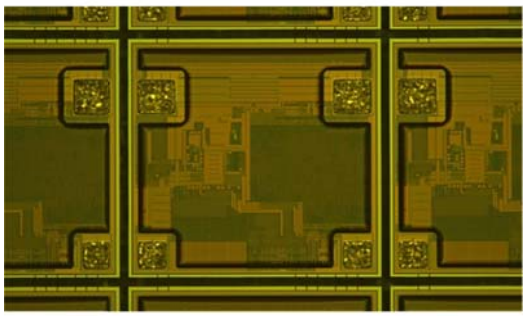


Abb. 49) Wafer Layout, Bare Die mit PIN Konfiguration[1)]; Wafer Detailansicht einer Chip Unterseite mit PADs

Auf der Unterseite befindet sich zwischen den Kontakt-Pads („Bumps") eine Distanzschicht (Spacer) aus 7µm Polyimid (PI), die dazu dient Toleranzen in der Bauteilhöhe auszugleichen. Weiterhin soll eine solche Unterfüllung, unter Temperaturbelastung auftretende Scherkräfte von den Bumps ableiten und aufnehmen[13)]. Die Kontakte mit einer Höhe von 18µm ragen dabei immer über diese Schicht heraus. Als Kontaktmaterial kommt bei diesem Typ reines (>99,9%) Gold zur Anwendung. Trotz der relativ hohen Temperaturbeständigkeit des PI-Kunststoffs von kurzzeitig bis +400°C, ist er für den XTC-ID Einsatz als kritisch anzusehen. Wie Materialuntersuchungen an nicht versiegelten XTC-ID TAGs zeigen, treten bei Temperaturen ab +550°C Spannungen und Scherkräfte in der Polyimid-Schicht auf, die eher an einen Glasbruch erinnern (Abb. 50-51) und oftmals zu einem Chipdefekt führen. In diesem Fall leitet die Unterfüllung die aufgenommenen Kräfte in das Silizium-Substrat weiter (Abb. 52). Die Exemplar Streuung zwischen einzelnen Chips ist dabei unerwartet hoch. Einige Exemplare zeigten bei Hot-Stage Mikroskopie Untersuchungen (Abb. 53) selbst bei Temperaturen bis 700°C keine sichtbaren Defekte und blieben voll funktionsfähig.

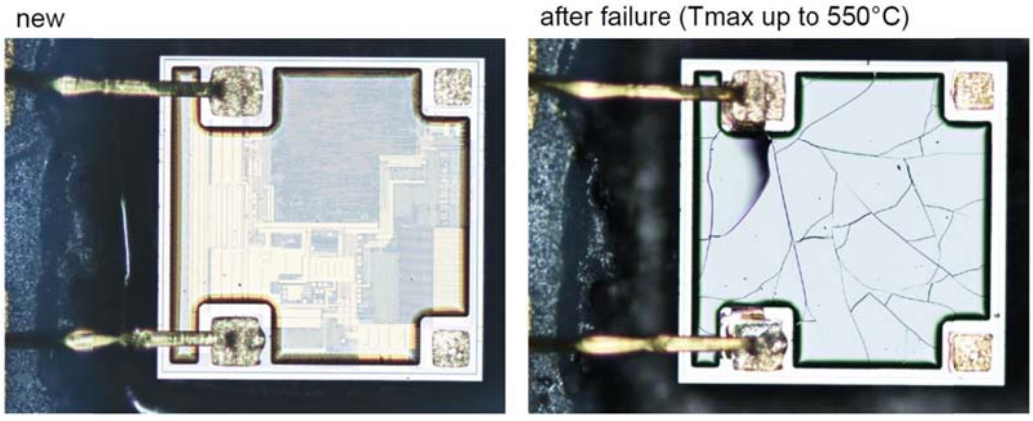


Abb. 50) Unterseite eines kontaktierten XTC-ID Chips vor (links) und nach (rechts) Temperatureinwirkung

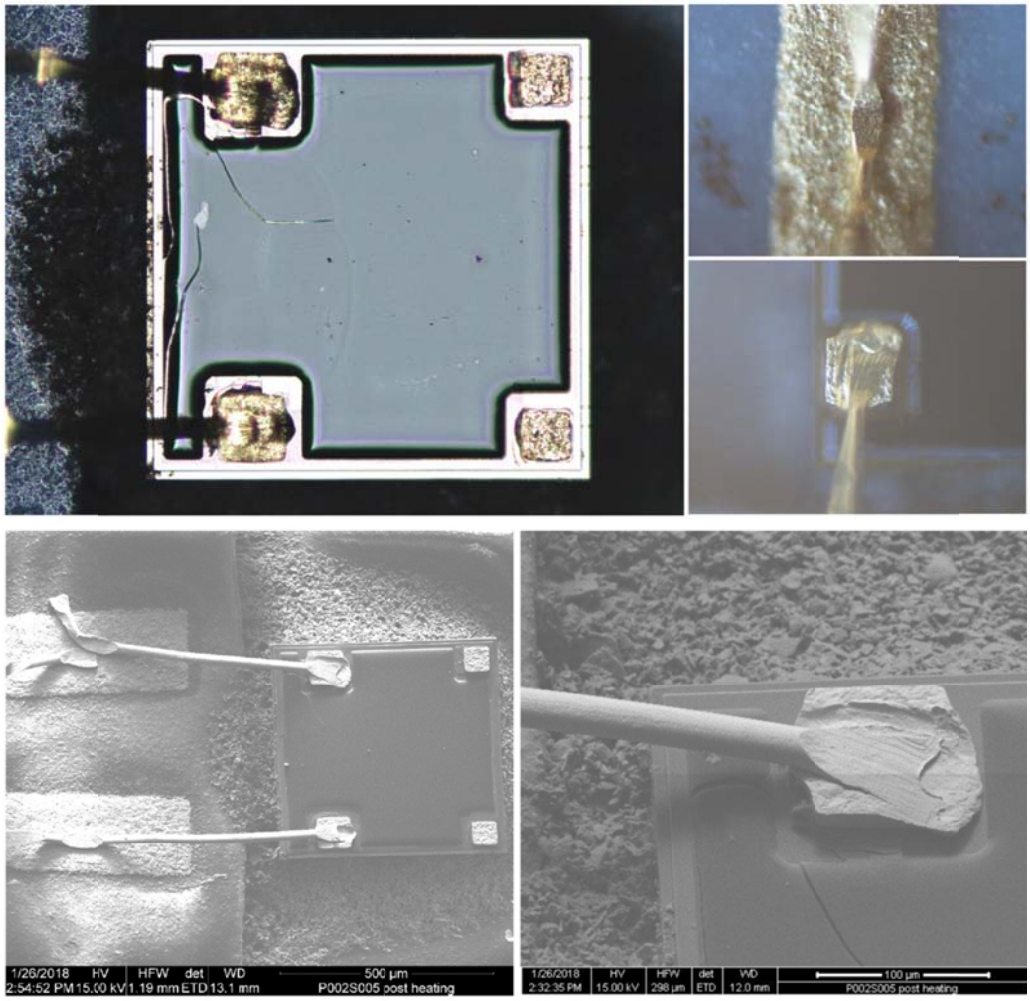


Abb. 51) Mikroskopische Untersuchung an der Chipunterseite auf sichtbare Risse und Defekte

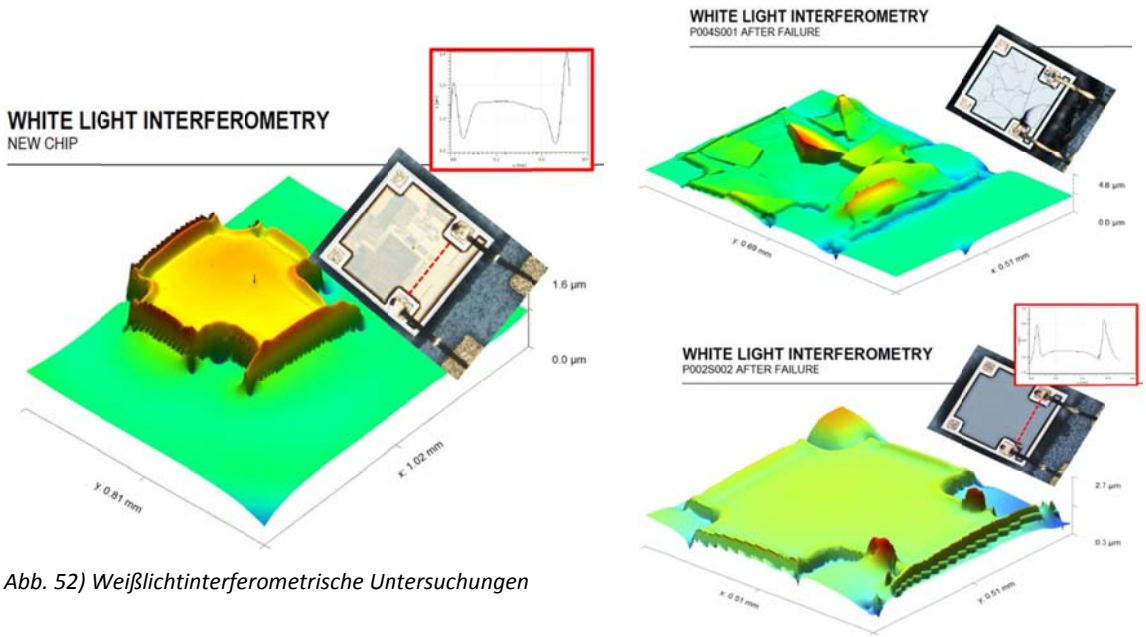


Abb. 52) Weißlichtinterferometrische Untersuchungen

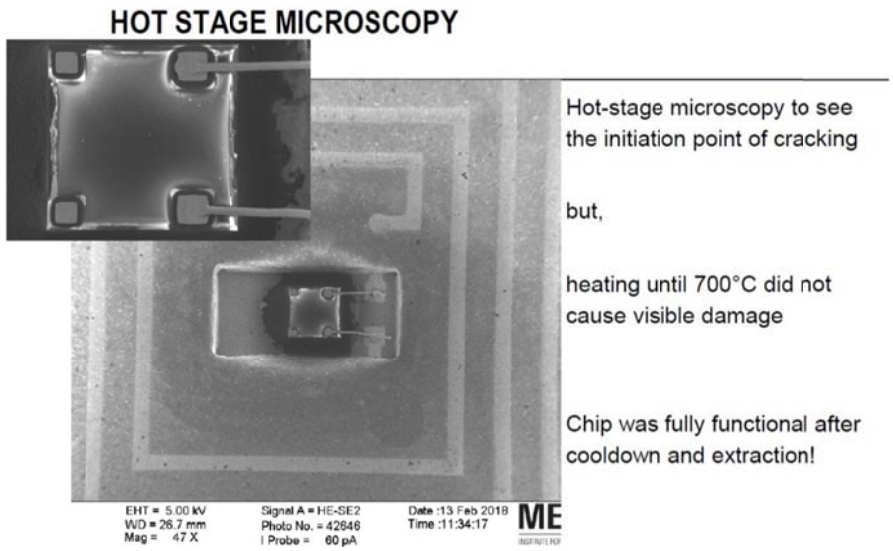


Abb. 53) Hot-Stage Mikroskopie Untersuchungen bis +700°C

Basierend auf diesen Ergebnissen, wurden typische Fehlerquellen festgestellt, die zu einem optimierten Chip Handling führten. Da die Polyimid Unterfüllung am Chip ab ca. 300°C Ausgasungs- und bei noch höheren Temperaturen Zersetzungserscheinung zeigt, wurden im XTC-ID TAG alle Chips vor ihrer Assemblierung künstlich gealtert und anschließend auf eine fehlerfreie Funktion hin getestet. Aufgrund der hohen chemischen Beständigkeit, waren Versuche zur Entfernung der PI-Unterfüllung mittels Lösungsmitteln wie Dimethylformamid (DMF) oder N-Methyl-2-pyrrolidon (NMP) nur bedingt erfolgreich. Wie Abbildung 54 zeigt, gelang zwar die chemische Entfernung der opaken Polyimid Schicht vollständig, jedoch kam es zur Beschädigungen der Struktur durch das Lösungsmittel. Erkennbar an den lilafarbenen Zonen im rechten oberen Ausschnitt. Für eine zukünftige TAG Produktion wird deshalb eine kundenspezifische Wafer Variante ohne PI-Unterfüllung angestrebt.

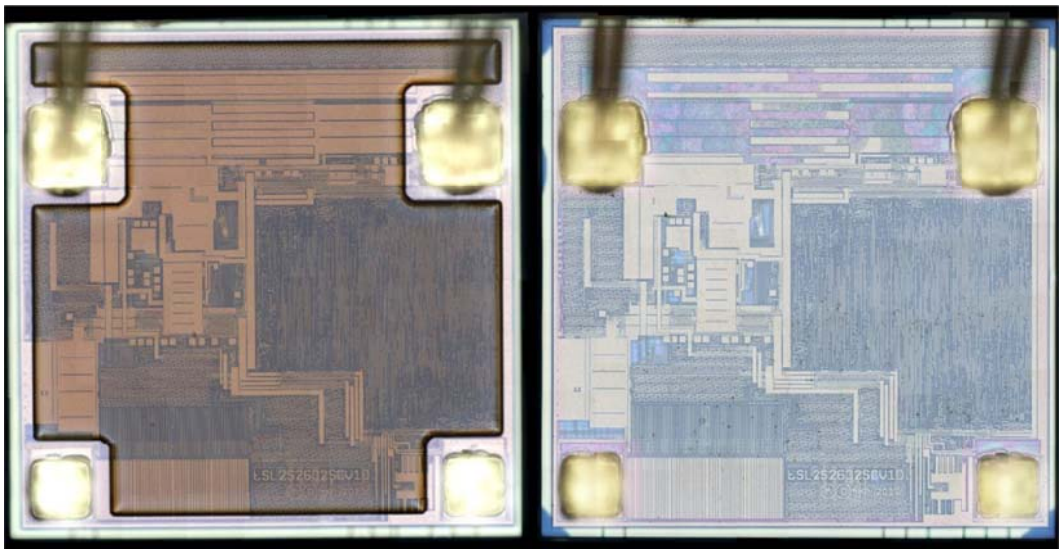


Abb. 54) chemische Entfernung der opaken Polyimid-Schicht (rechts unbehandelt, links chemisch entfernt)

3.4 nano-Silber Sinterpasten vs. Drahtbonding

Zur Kontaktierung zwischen Chip und RFID-Antenne wird standardmäßig ein Drahtbonding Verfahren mit Flip-Chip Technik innerhalb der Cavity angewandt (Abb. 55). Dazu wird ein dünner Metalldraht aus einem, zu den Kontaktstellen passenden Material (häufig eine Goldlegierung), untereinander punktförmig verschweißt. Der Chip wird dabei auf die Oberseite gedreht (Flip-Chip), so dass die entsprechenden Pads zugänglich werden und dabei mit wenig Arcylatkleber fixiert. Vorteil dieser Technik ist die Abwesenheit anderer chemischer Verbindungen, wie Flussmittel, Haftvermittler usw. in den Kontaktstellen, da nur gleichartige reine Metalle miteinander „verschmolzen“ werden (Abb. 56). Nachteilig wirken sich dagegen die fragile, erschütterungsempfindliche Struktur sowie der hohe manuelle Arbeitsaufwand aus. Zudem muss beim XTC-ID TAG der vorher aufgebrachte Kleber, durch eine weitere Temperaturbehandlung zersetzt und ausgetrieben werden, bevor die Cavity versiegelt werden kann. Auch dieser letzte Schritt muss händisch erfolgen, damit eine Unterfüllung und vollständige Einbettung des Bonddrahts in das Keramikmaterial gewährleistet ist. Infolge des komplexen Arbeitsaufwandes, der sich für eine Massenfertigung nur schwer automatisieren lassen wird, wurden im Projektverlauf ebenfalls alternative Verfahren zur Kontaktierung evaluiert.

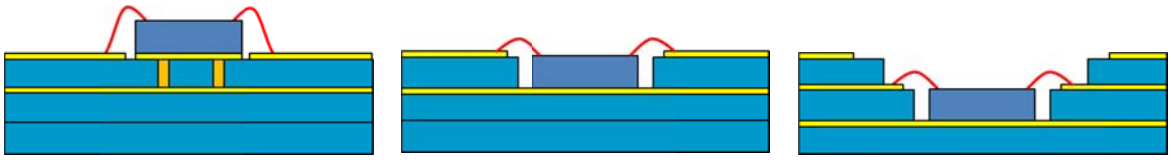


Abb. 55) Bonding Möglichkeiten zur Flip-Chip Montage (XTC-ID TAG rechte Variante in Cavity)

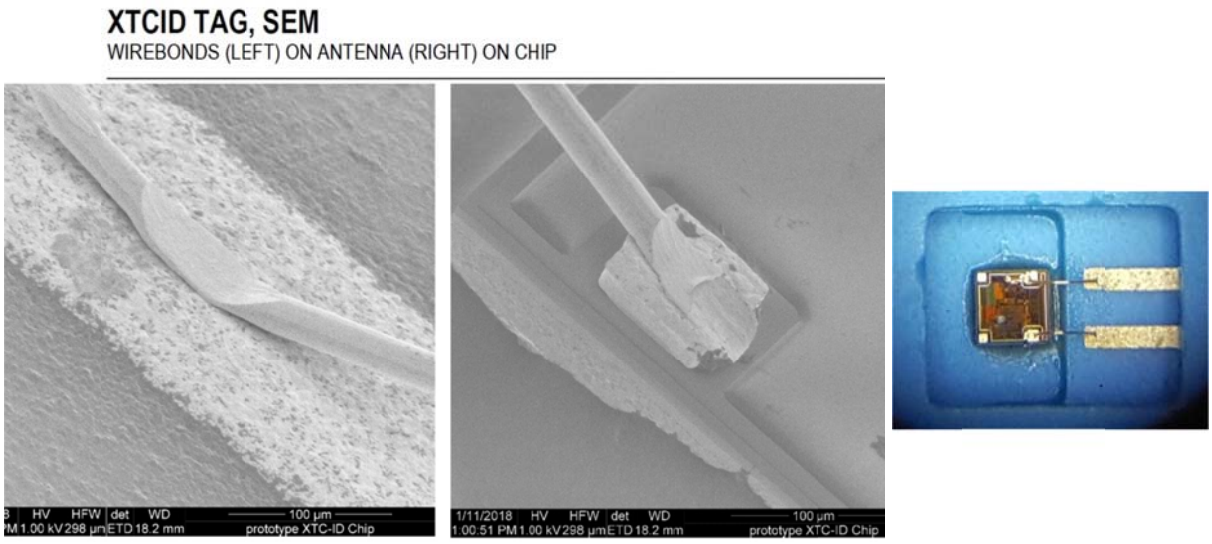


Abb. 56) SEM-Aufnahmen der Drahtbonding Kontaktpads im XTC-ID TAG, mikroskopische Teilansicht der Cavity (rechts)

Aufgrund erster Ergebnisse der Materialuntersuchungen an gebondeten XTC-ID Prototypen bei tiefen Temperaturen, wurde die Suche nach alternativen Kontaktierungsverfahren intensiviert. Alle gemessenen Muster zeigten bei -190°C (LN_2) einen Totalausfall infolge beschädigter Bondkontakte,

unabhängig davon, ob die Cavity offen oder mit einer keramischen Unterfüllung versiegelt war. Die auftretenden mechanischen Spannungen beim Abkühl- bzw. Auftauvorgang sind deutlich größer, als die Fügekräfte der Metallschmelze, wodurch es auf mikroskopischer Ebene zu einem Abriss des Bonddrahtes unter Kontaktverlust kommt.

Gesucht wurde eine Lötpaste, die eine Oberflächenmontage (SMD) des Chips ermöglicht und dabei einen Schmelzpunkt von mindestens +500°C besitzt, um eine temperaturbeständige Lötstelle zu gewährleisten. Herkömmliche Lötpasten kommen nicht in Frage, da ihre Schmelzpunkte typischerweise um die ~320°C liegen, während die danach folgenden Silberlote eine Löttemperatur nahe dem Schmelzpunkt von Silber (+961°C) benötigen und demzufolge ebenfalls nicht in Frage kommen. Dieses anscheinend unlösbare Paradoxon, lässt sich aber mit Hilfe der nano-Technologie und neuartigen Organometall Verbindungen lösen. Das Konzept ähnelt dabei in gewisser Weise dem Ansatz bei den LTCC-Folien (Kap. 3.2.1). Die Organometall Verbindung besteht hier aus einem Silber nano-Partikel als Koordinationszentrum, das mit mehreren organischen Resten, vornehmlich aromatischen Ringstrukturen, verknüpft ist. Die Zugabe von einem geeigneten Lösungsmittel erlaubt die Einstellung der Viskosität zu einer stabilen Sinterpaste und verhindert zudem eine Aggregation (Zusammenballung) der Teilchen. Trotz des hohen elementaren Silberanteils in der Sinterpaste, bewirken die organischen Reste im Molekül einen drastischen Abfall des Schmelzpunktes auf nur noch +230°C, bei gleichzeitiger Zersetzung des organischen Anteils in gasförmige Stoffe. Es kommt dabei zur Abscheidung der nano-Silberpartikel, unter gleichzeitiger Ausbildung einer elementaren Silberschicht an den Kontaktflächen (Abb. 57). Für den Praxiseinsatz heißt das, ein einmaliger Sinterprozess bei gemäßigten Temperaturen von ca. +250°C, führt zu einer Lötstelle aus elementarem Silber mit einem Schmelzpunkt von +961°C, ohne das je ein Bauteil dieser Temperatur ausgesetzt war (Abb. 58). Der Sinterprozess ist analog zum gängigen Reflow-Löten, ohne externe Druckbeaufschlagung oder Bauteilfixierung unter Atmosphärendruck möglich.

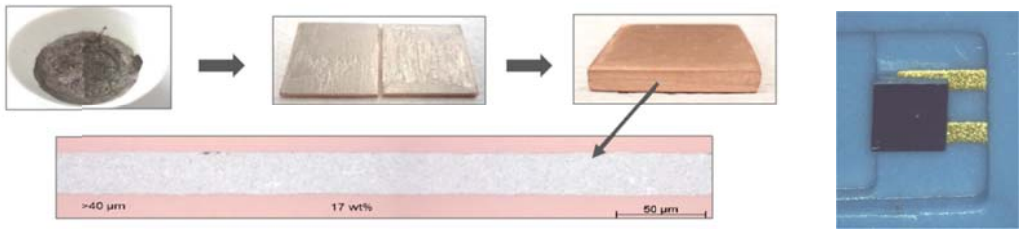


Abb. 57) nano-Silber Organometall Sinterpaste[14)],

Sinterversuch am XTC-ID Chip

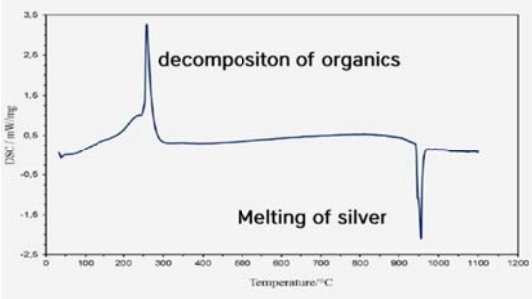
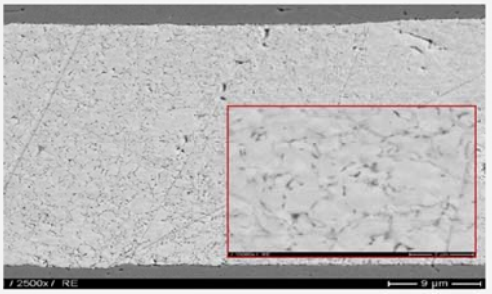


Abb. 58) Temperaturbeständigkeit der Sinterpaste,



elementare Silberschicht nach dem Sinterprozess

3.5 XTC-ID TAG (Aufbau & Eigenschaften)

Der XTC-ID TAG wurde während der Entwicklungsphase kontinuierlich optimiert und durchlief dabei drei Evolutionsstufen. Neben den angestrebten Spezifikationen, wie eine hohe Temperaturbeständigkeit und Inertheit, zeichnet er sich insbesondere durch eine große Flexibilität in der Chip Bestückung aus. Das Design ist so universell, dass auch ein späterer Wechsel auf eine andere RFID-Technologie, wie beispielsweise dem UHF Frequenzband, mit relativ geringem Aufwand zu bewerkstelligen ist. Der Substrataufbau erfolgte im Mehrschichtverfahren aus vier Lagen LTCC-Tape, mit jeweils separat aufgedruckten, elektrisch leitfähigen Strukturen aus Gold (Tab. 8).

Layer Nr.	Name	Funktion	Material	Tool	Dicke [µm] (green)	Dicke [µm] (co-fired)	Info	Stapel-Richtung
4	C04-T	Conductor	5739	screen				
4	S04	Dielectric substrate	DP951	punching	165	140	Vias	90° ↑
4	V04	Via Layer	5738R	stencil				
3	C03-T	Conductor	5742 Au	screen				
3	S03	Dielectric substrate	DP951	punching	165	140	Vias	0° →
3	V03	Via Layer	5738R	stencil				
2	C02-T	Conductor	5742 Au	screen				
2	S02	Dielectric substrate	DP951	punching	165	140	Vias	90° ↑
2	V02	Via Layer	---	---			no print	
1	C01-T	Conductor					no print	
1	S01	Dielectric substrate	DP951	punching	165	140	Cavity	0° →
1	V01	Via Layer					no print	

Tab. 8) LTCC-Lagenaufbau im XTC-ID TAG (no print = keine Leiterbahnen oder Pads in diesem Layer)

Nach dem Sintern der Substrate mit dem Temperaturprofil aus Abbildung 38, zeigten die elektrischen Messungen eine gute Qualität mit geringer Toleranz in der Induktivität (L) der Antennenstruktur. Die gemittelten Messwerte betrugen für R = 476 Ω (±1 Ω) und L = 5,6 µH (±0,1µH). Das TAG Layout zusammen mit einer 3D-Ansicht der verschiedenen Bestückungsvarianten innerhalb der Cavity, wird in den Abbildungen 59-60 gezeigt.

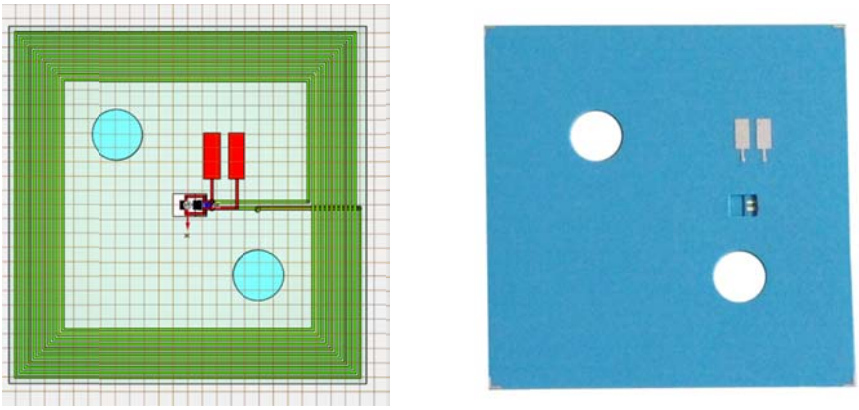


Abb. 59) Layout und Originalansicht vom XTC-ID TAG

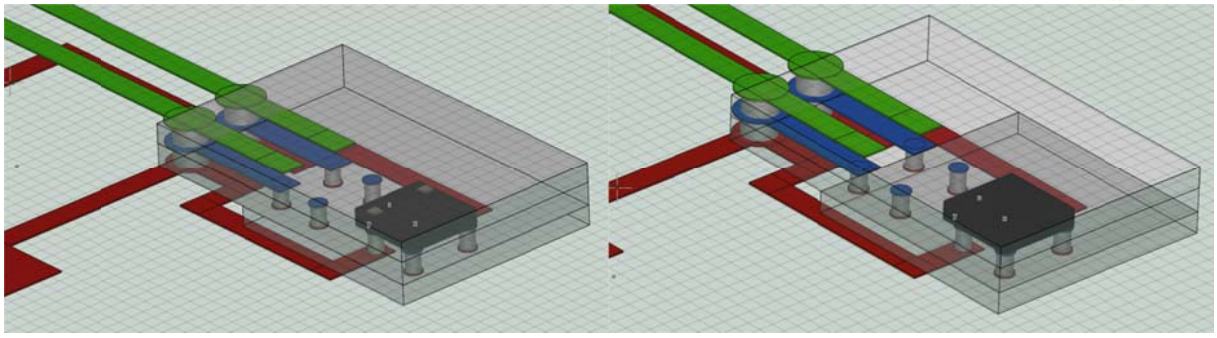


Abb. 60) 3D-Ansicht der Cavity, Flip-Chip Montage mit Bonding (links) und SMD Montage mit Sinterpaste (rechts)

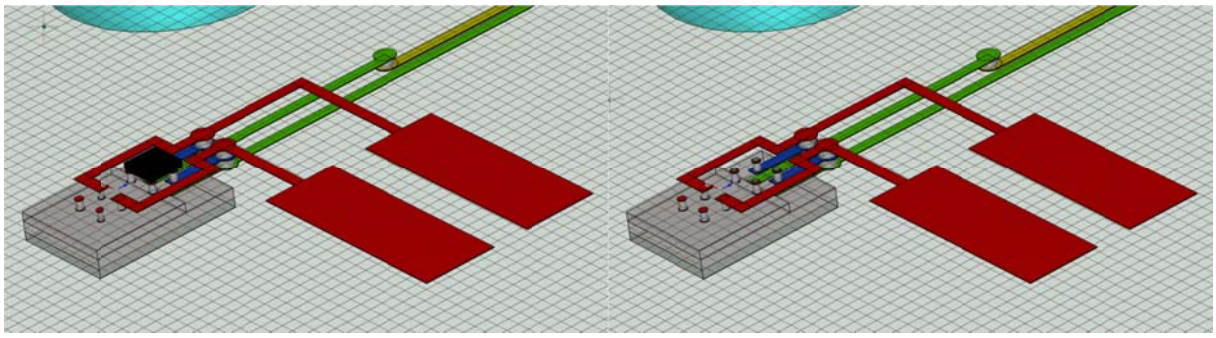


Abb. 61) SMD-Version außerhalb der Cavity (links) und Funktion als RFID-Antenne unbestückt (rechts)

Die Chipmontage kann für spezielle Anwendungsfälle ebenfalls außerhalb der Cavity, in Form einer kostengünstigen SMD Version, ausgeführt werden. Als unbestückte Variante oder bei einem defekten Chip ist es weiterhin möglich, den TAG als temperaturbeständige RFID-Antenne weiter zu verwenden. Dazu ist an den rot markierten Kontakten (Abb. 61) der nach außen geführten Antenne eine, entsprechend der zu erwartenden Temperaturbelastung geeignete Kabelverbindung anzuschließen. Beide Kontakte können weiterhin als „Erdung“ fungieren, um beispielsweise eine Überspannung durch starke äußere elektromagnetische Felder (z.B. Mikrowelle), während Transport und Lagerung abzuleiten. Der Kontaktschluss kann in diesem Fall auch durch einfache Federkontakte innerhalb einer Halterung erfolgen. Allerdings muss in diesem Fall, bei einem Lese- oder Schreibzugriff der TAG vorher entnommen werden.

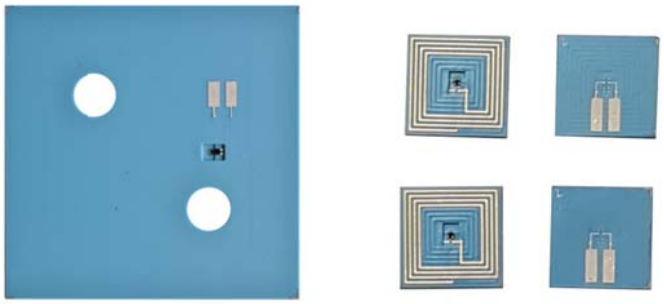


Abb. 62) separate Antennenpads im XTC-ID TAG in zwei Formaten

Ergänzend sei erwähnt, dass zum Aufbau des Substrats die bleihaltige LTCC-Folie Dupont 951-AX verwendet wurde. Die damit hergestellten Prototypen sind demzufolge nicht ROHS konform und

somit nur für den industriellen Einsatz vorgesehen. Bei einer zukünftigen Produktion wird dieses Material durch einen bleifreien Typ ersetzt, wodurch der TAG die ROHS-Norm erfüllt und sodann auch für andere Applikationen geeignet ist (siehe Datenblatt in Anhang B).

Wie alle Silizium Halbleiter hat auch der XTC-ID TAG eine maximale Betriebstemperatur von ca. +152°C. Oberhalb dieser Schwelle ist eine Lese- oder Schreibfunktionalität nicht mehr möglich, da die Gitterschwingungen im Siliziumkristall eine geordnete Elektronenbewegung blockieren. Dazu sind in Abbildung 63 die Temperaturkurven mehrerer Aufheiz- und Abkühlzyklen bei zwei unterschiedlichen Temperaturprogrammen dargestellt. Die rot markierten Kurvenverläufe an den unteren Scheitelpunkten zeigen deutlich das Ende und die Wiederaufnahme der Betriebsbereitschaft bei einer Bereichsschwelle von +152°C (±2°C). Interessanterweise liegen die Schwellenwerte der Wiederaufnahme in den Abkühlkurven (resume ▲ und ▲) immer deutlich oberhalb der Toleranzschwelle.

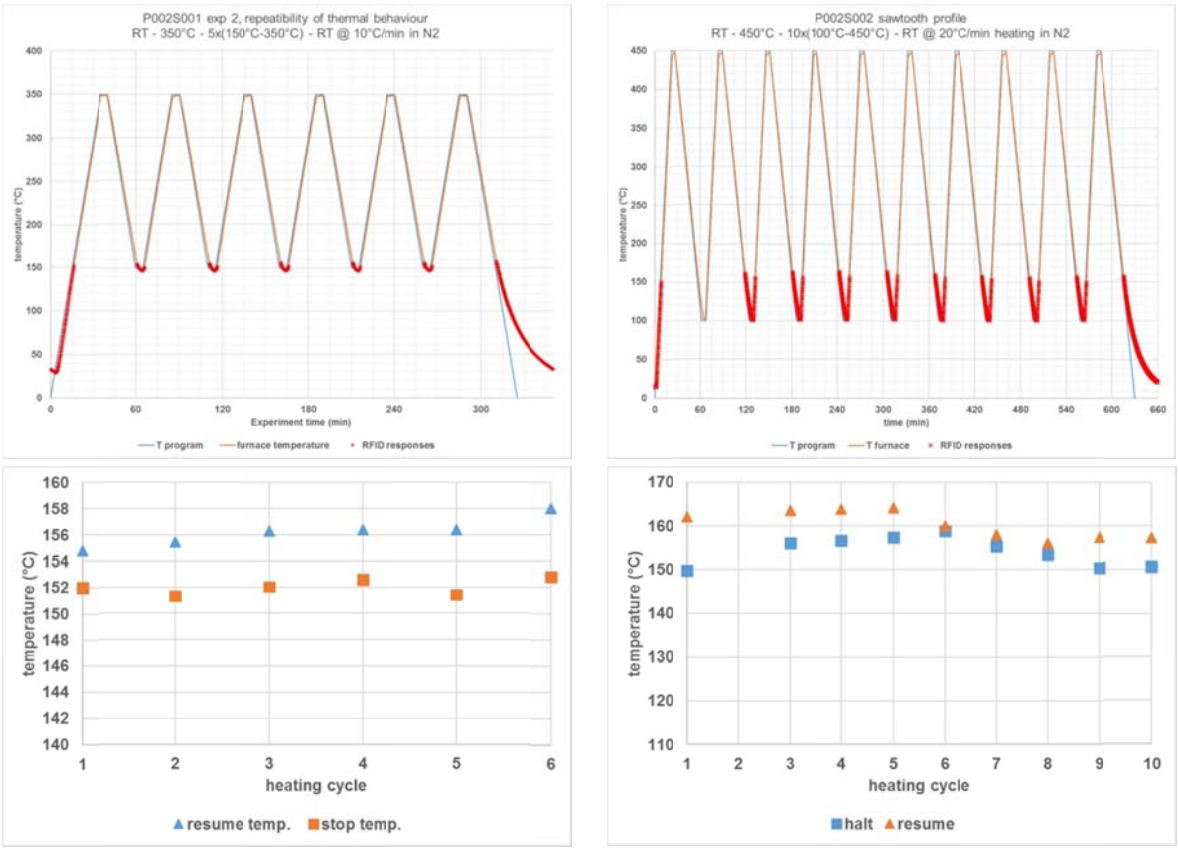


Abb. 63) Temperaturprogramm mit Heiz- und Kühlkurven mehreren Zyklen (rote Markierung zeigt Betriebsbereitschaft)

Der Datenerhalt im EEPROM-Speicher ist aber bis zu einer Lagertemperatur von +450°C sichergestellt, wobei sich nach einer Temperaturbelastung ab +400°C, eine Aktualisierung des kompletten Speicherinhalts („refresh“) von Zeit zu Zeit empfiehlt. Ebenso bietet sich hier der Einsatz eines Fehlerkorrektur Algorithmus im Kommunikationskanal zwischen TAG und Reader an. Oberhalb dieser Temperaturschwelle kommt es statistisch gesehen zu einer Häufung sogenannter „bit-flips“, der zufälligen Änderung eines Bits im EEPROM Speicher. Infolge des Fowler-Nordheim-Tunneleffektes erfolgt dabei ein Wechsel im Bit Wert immer von eins nach null, da die benötigte

Austrittsarbeit in höheren Energieniveaus (eins) geringer ist als im Grundzustand (null) und damit die Wahrscheinlichkeit steigt, dass durch Zuführung von thermischer Energie ein Elektron den Potentialwall durchdringen (tunneln) kann. Für solch ein Testverfahren wurden zunächst alle Speicherzellen mit dem hexadezimalen Wert 7E (Bitfolge 111 1110) bzw. FF (Bitfolge 111 1111) kodiert (Abb. 64 linke Darstellung). Nach mehreren Heizzyklen mit maximal Temperaturen bis +450°C wurde der Speicher erneut ausgelesen. Nach der statistischen Auswertung[15)] kam es bei ~10% der Testmuster zu einem oder mehreren bit-flips, wobei das Ergebnis eine signifikante Temperatur-abhängigkeit von der verwendeten Maximaltemperatur zeigt. In der rechten Darstellung (Abbildung 64) wechselt beispielsweise im Speicherblock 07 das zweite Byte zu hexadezimal 6E (Bitfolge 110 1110) sowie im Block 13 ebenfalls das Byte Nummer 2 zu hexadezimal 7A (Bitfolge 111 1010). Die Position sowie die Anzahl an „defekten“ Speicherzellen mit bit-flip Effekt, ist statisch verteilt und nicht vorhersehbar. Allerdings zeigen die Speicherzellen, auch nach einer Neuprogrammierung mit anschließendem Temperaturzyklus, häufig an der gleichen Position einen Bitfehler, was auf eine Schwächung in der internen Halbleiterstruktur infolge von Exemplar Streuungen hindeutet. Eine Qualitätskontrolle der Chips nach einer künstlichen Alterung, kann diesen Effekt dabei zumindest teilweise begrenzen. Die in Kapitel 3.3 beschriebenen Chips mit F-RAM Speichertechnologie werden dagegen voraussichtlich noch robuster gegen diese Fehlerquelle sein. Es ist zu erwarten, dass ihr Einsatz den Arbeitsbereich zu höheren Temperaturen hin erweitern wird.

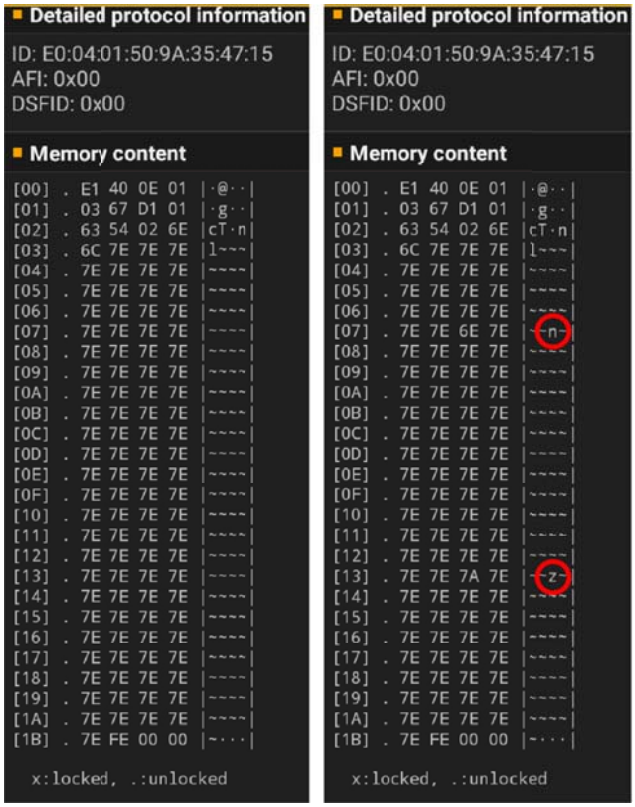


Abb. 64) Bit-Flips im EEPROM Speicher (rote Markierung) nach zyklischer Temperaturbehandlung

4. XTC-ID Reader

4.1 Hardware Beschreibung

Im Rahmen des Projektes wurde weiterhin die Entwicklung einer innovativen und modularen RFID-Reader Hardware umgesetzt. Dabei wurde schon während der Konzeptionsphase großen Wert auf Alleinstellungsmerkmale gelegt, um Interessenten auch zukünftig eine skalierbare Plattform bieten zu können. Neben der Integration von 25 internen Antennen mittels Antennenumschalter, zählen dazu besonders die Implementierung eines LAN-Moduls, als weitere Kommunikationsschnittstelle neben dem Mini-USB Port sowie die Möglichkeit auch sechs externe Antennen mit eigener Abstimmungselektronik über Stecksockel anzubinden. Gerade die Flexibilität im Design, erlaubt auch weiterhin Änderungen für neue Applikationen, wie beispielsweise der Medizintechnik.

Der XTC-ID Reader in seiner aktuellen Ausbaustufe v.3.0, arbeitet im HF-Band bei 13,56 MHz. Für die Kompatibilität nach dem NFC Standard sorgt ein NXP PN7120/PN7150 Halbleiter[16)], der die grundlegende Lese-/Schreibfunktionalität durch seine integrierte Firmware zur Verfügung stellt. Neben typischen NFC TAGs werden zudem auch andere ältere HF-TAGs nach ISO/IEC 14443 Norm unterstützt (Abb. 47). Der XTC-ID Reader kann entweder über das serielle RS-232/USB Interface, wie auch über die eingebaute LAN-Schnittstelle mit einem anderen Terminal (Endgerät) kommunizieren. Hierzu werden reine ASCII-Text Steuerbefehle benutzt (siehe Kapitel 4.2).

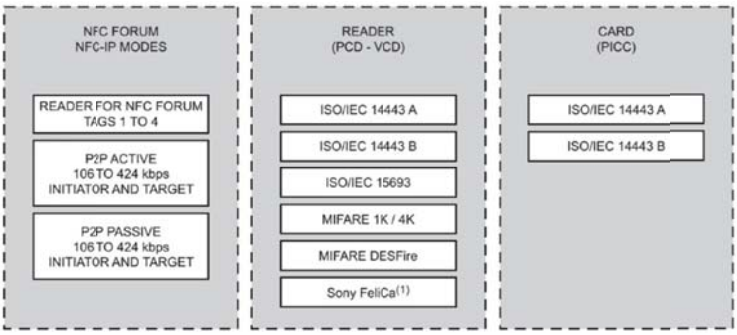


Abb. 65) PN7120/PN7150 unterstützte Übertragungsstandards

Alle Funktionen befinden sich auf einer einzigen mehrlagigen Leiterplatte (PCB), die sich einfach in Laborgeräte wie z.B. chemische Analysegeräte oder anderen Industrieanlagen integrierten lässt. Dazu wurde die Leiterplatte je nach Applikation, für zwei unterschiedliche Bestückungsvarianten ausgelegt.

1) <u>Variante A</u>
   Antennenarray mit 25 gedruckten Antennen im Raster 5×5 für 2ml Vials (Laborautomation). Optional kann das Antennenarray vom Logikteil an der weißen Schnittlinie vertikal getrennt werden, um beispielsweise eine geeignete Platzierung in vorhandene Gehäuse zu ermöglichen. Anschließend müssen die Verbindungen SW1 (Antennenschalter Ansteuerung), SW2 (HF-Signal) sowie 3.3V/DC und GND (In/Out) nach Abbildung 66 verbunden werden.

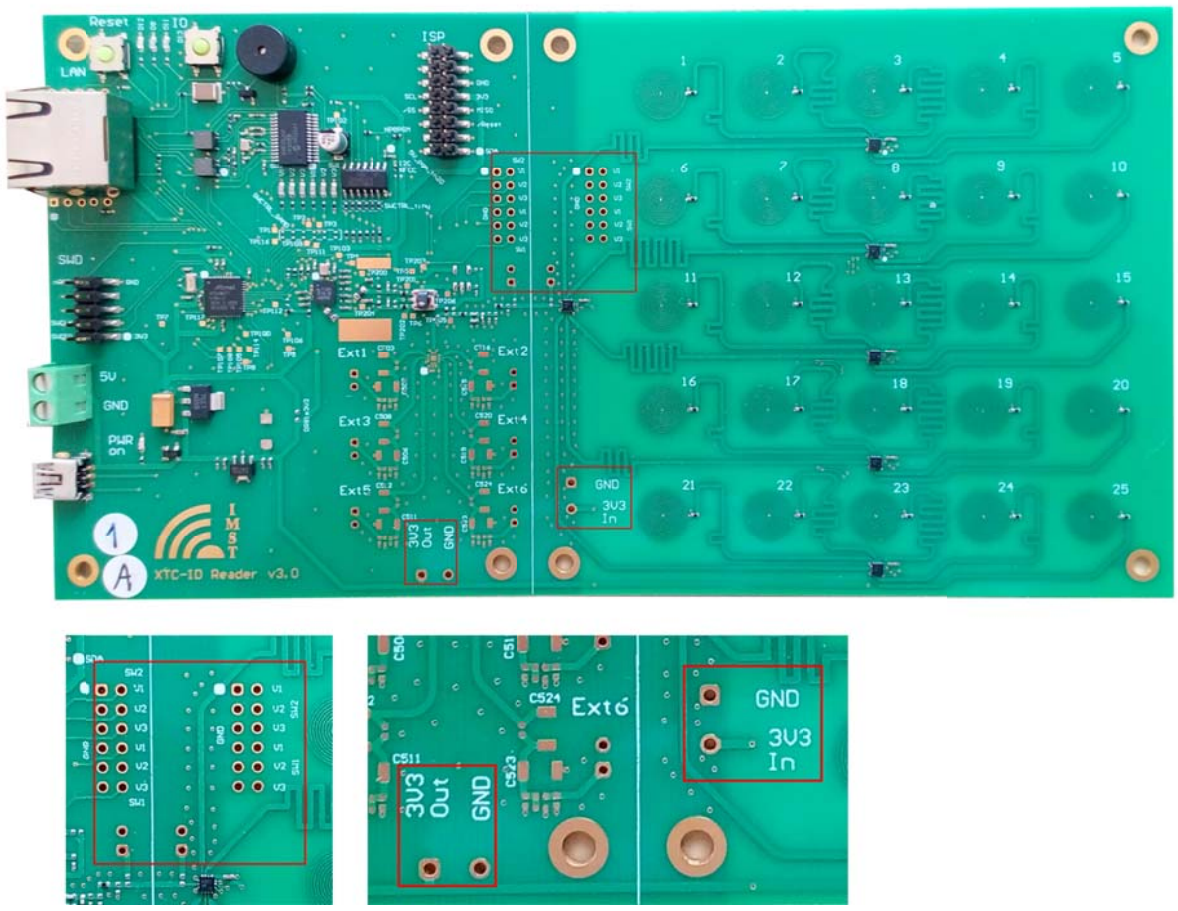


Abb. 66) XTC-ID Reader Variante A mit 25fach Antennenarray (markierte Verbindungen bei Trennung kontaktieren)

2) <u>Variante B</u>

Sechs externe Antenneneingänge EXT1 – EXT6 mit jeweils eigener Abgleichmöglichkeit über zwei Trimmkondensatoren (Abb. 67**)**. Optional kann die Leiterplatte an der weißen vertikalen Schnittlinie getrennt werden um Platz zu sparen. Folgender Stecker-Typ wurde verbaut:
TE Connectivity / Antennenstecker Nr. 1744417-2 / Crimp-Kontakte Nr.: 2232983-1

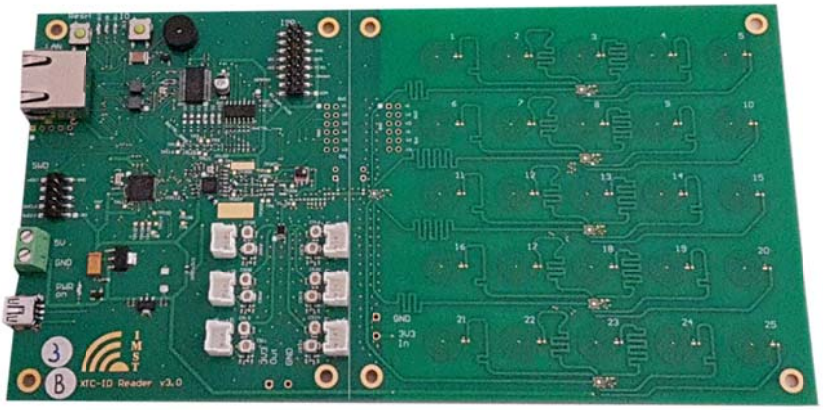
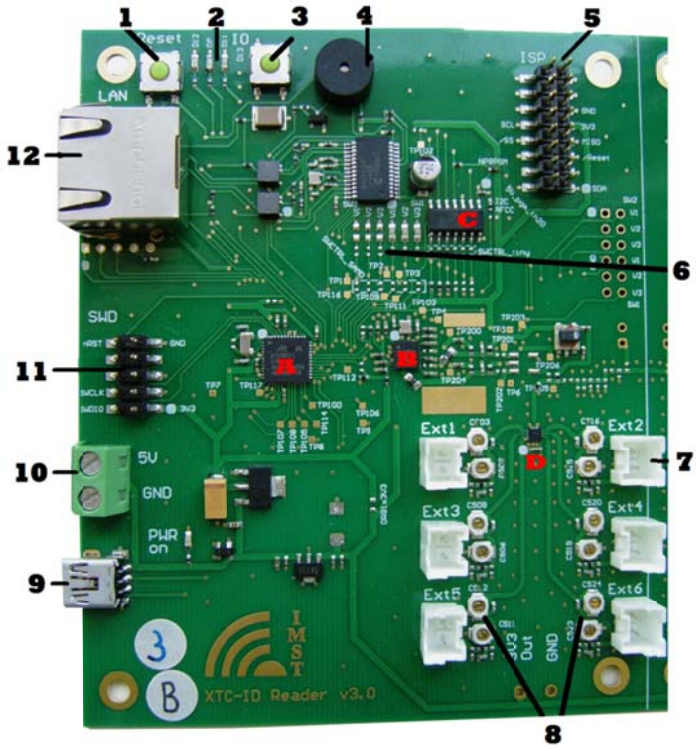


Abb. 67) XTC-ID Reader Variante B mit 6 externen Antenneneingängen

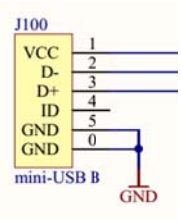
Die Lage aller zum Betrieb notwendigen Anschlüsse und Funktionselemente auf dem Logikboard kann der nachstehenden Abbildung 68 entnommen werden.



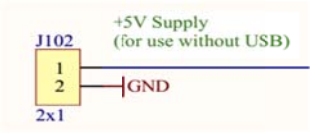
Nr.	Funktion
1	Reset & Firmwareupdate
2	TAG Status LEDs (D12, D9, D11)
3	Funktionstaste (ASS Ende)
4	Signalgeber (TAG Erkennung)
5	Slave Controller I²C-Interface
6	LEDs der RF-Switch Kodierung
7	externe Antenneneingänge (1…6)
8	Trimmkondensatoren zum Antennenabgleich (zwei pro Port)
9	mini-USB Buchse für Versorgungsspannung & Datenübertragung
10	separater, optionaler Eingang für Versorgungsspannung (5V/DC)
11	Debug Interface Hauptcontroller
12	LAN/Ethernet Schnittstelle
13	LED Einschaltanzeige (PWR on)
A	Atmel ARM ATSAM D21 CPU
B	NXP 7120 RFID-Reader Chip
C	ATtiny20 RF-Switch Controller
D	SP6T HF-Switch

Abb. 68) XTC-ID Reader Logikboard mit Bauteilübersicht

4.1.1 USB-Schnittstelle & Versorgungsspannung



(**9**)



(**10**)

Die standardmäßige mini-USB 2.0 Buchse (**9**) dient sowohl der Datenkommunikation mit einem Endgerät, im einfachsten Fall beispielsweise einem PC mit Terminalprogramm sowie gleichzeitig der Stromversorgung. Mit einer 5V/DC Gleichspannung und einer maximalen Leistungsaufnahme von 100mA liegt der Energiebedarf bei recht geringen 0,5 Watt im Dauerbetrieb. Durch den nachgeschalteten Spannungsregler arbeitet die Elektronik intern mit 3,3V Betriebsspannung. Eine aktive Kühlung der Komponenten ist nicht erforderlich. Optional ist die Zuführung der Versorgungsspannung auch über ein externes Netzteil möglich. Der Netzteilausgang mit 5V geregelter Gleichspannung, wird unter Berücksichtigung der Polarität dazu an die zweipolige Schraubklemme (**10**) angeschlossen. Diese Variante bietet sich insbesondere bei einer Nachrüstung in bestehende Geräte oder bei Verwendung der integrierten LAN-Schnittstelle (**12**) an. Das Anliegen einer korrekten Versorgungsspannung, wird hier durch die grüne Power on LED (**13**) signalisiert.

Nach der erstmaligen Herstellung einer USB-Verbindung mit einem PC, wird unter Windows 10 als Betriebssystem automatisch der richtige Treiber installiert. Sollten hierbei Probleme auftreten oder ein älteres Betriebssystem mit Windows 7/8 vorliegen, stehen die Adafruit Windows Treiber samt Quellcode auch im Internet zum Download[17)] bereit. Der USB Anschluss ist anschließend als virtuelle serielle Schnittstelle im Windows Gerätemanager unter COM-Ports zu finden (Abb. 69). Die zugewiesene COM-Port Nummer ist sodann unter den Verbindungseinstellungen einer entsprechenden Kommunikationssoftware einzutragen.

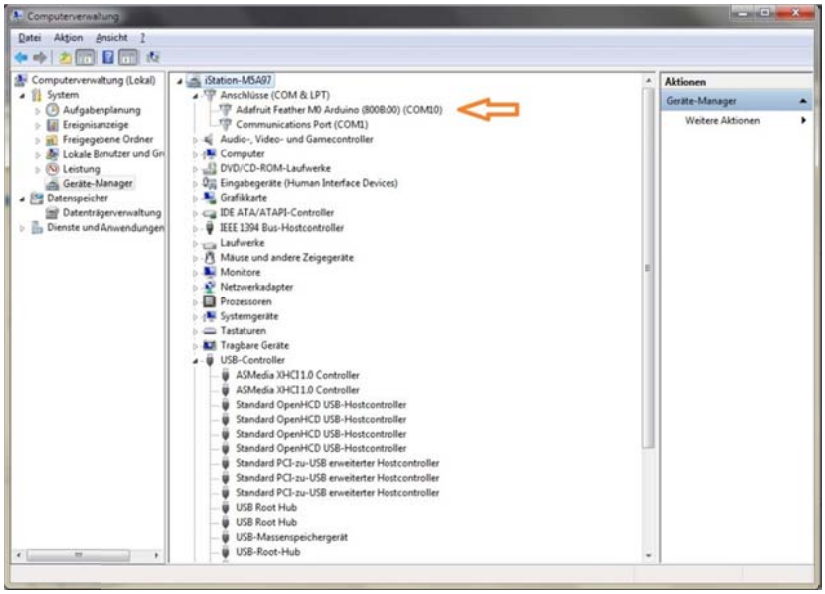


Abb. 69) Gerätemanager mit registriertem USB Treiber als COM10 (hier Windows 7)

ACHTUNG

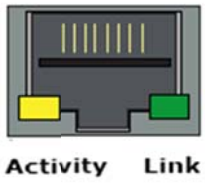
Die Zuweisung einer Port Nummer gilt nur für diesen einen physikalischen USB-Anschluss am PC. Wird das Kabel an einen anderen USB-Anschluss gesteckt, ändert sich die COM-Nummer entsprechend! Gleiches gilt für ein Firmware Update, wobei hier grundsätzlich ein anderer COM-Port verwendet wird.

TIP

Eine Funktionsprüfung von XTC-ID Reader und TAG lässt sich auch ohne PC oder anderen Endgeräten einfach durchführen. Dazu ist der Reader nur an eine 5V/DC Versorgungsspannung anzuschließen. Nach dem Booten und ohne aktive Datenkommunikation ist standardmäßig in allen Reader Varianten Antenne Nummer eins [1] aktiv und wird dreimal pro Sekunde zyklisch abgefragt (Continuous Detection Mode). Sobald ein TAG im RF-Feld dieser Antenne einwandfrei erkannt und die ID fehlerfrei ausgelesen wurde, ertönt parallel zum Abfrageintervall ein Signalton (Beep). Diese Programmschleife wird automatisch nach der ersten Aufnahme einer Datenverbindung beendet.

4.1.2 LAN-Schnittstelle

Der XTC-ID Reader ist neben der USB- auch mit einer LAN-Schnittstelle (**12**) für TCP/IP Netzwerke ausgerüstet. Verbaut wurde ein Ethernet IC vom Typ ENC28J60T (Microchip Technology), welches die seriell anfallenden Daten nach dem TCP/IP Protokoll konvertiert. Die Ethernet Geschwindigkeit beträgt 10/100 Mbps (auto-negotiate, auto-sense) und unterstützt automatisch den Full- oder Half-Duplex Modus. Die RJ-45 Buchse ist mit zwei verschieden farbigen LEDs ausgestattet, die den aktuellen Schnittstellenzustand nach Einstecken eines LAN-Kabels signalisieren (Tab. 9). Für die Erstinbetriebnahme sind die zugehörigen Konfigurationsdaten (IP Adresse, Subnetmask, Gateway, TCP-Portnummer) zuvor über die USB-Schnittstelle mit einem Terminalprogramm zu konfigurieren (siehe Kap. 4.2). Diese Konfigurationsparameter werden in einem nichtflüchtigen Flashspeicher abgelegt und stehen auch nach einem Stromausfall wieder zur Verfügung.



Label	Farbe	Port Status
Activity	gelb leuchtend	Link hergestellt, aber inaktiv
	gelb blinkend	Link hergestellt und aktiv
	aus	keine Ethernet-Verbindung
Link	grün leuchtend	Ethernet-Verbindung mit 100 Mbit/s
	grün blinkend	Ethernet-Verbindung mit 10 Mbit/s

Tab. 9) Status LEDs im RJ-45 Modulstecker

TIP

Die Art der vom Reader zu verwendenden Kommunikationsschnittstelle wird nach einem Reset eingestellt (beim Einschalten des Gerätes oder Drücken der Reset-Taste). Danach wird diejenige Schnittstelle ausgewählt, die als erste mit dem Reader kommuniziert. Die Auswahl einer anderen Schnittstelle ist erst nach einem erneuten Reset (**1**) möglich.

4.1.3 Debug-Schnittstellen (SWD & ISP)

Beide Schnittstellen sind als Pfostenstecker ausgeführt und nur für den internen Gebrauch bestimmt. Das Serial Wire Debug (SWD) Interface (**11**) stellt die Verbindung zum Hauptprozessor (**A**) her und wird zur Anpassung und Fehlersuche innerhalb der Firmware verwendet. Ein Firmware Update für den Anwender wird ausschließlich über die USB-Schnittstelle mit einem Updatepacket für den PC ausgeführt.

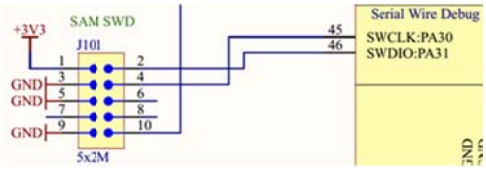


Abb. 70) Belegung der Serial Wire Debug (SWD) Schnittstelle

Über das Atmel Tiny Programming Interface (TPI) wird die verschlüsselte, werksseitige Programmierung der Antennenschalter Funktionalität für den ATtiny20 Prozessor (**C**) eingepflegt. Ein unsachgemäßer Zugriff auf diesen Port führt zu einem Hardwaredefekt verbunden mit einem Verlust der Garantieleistung. Der Pfostenstecker (**5**) beinhaltet ebenfalls Signalleitungen für die internen SPI und I^2C Bussysteme (Abb. 71).

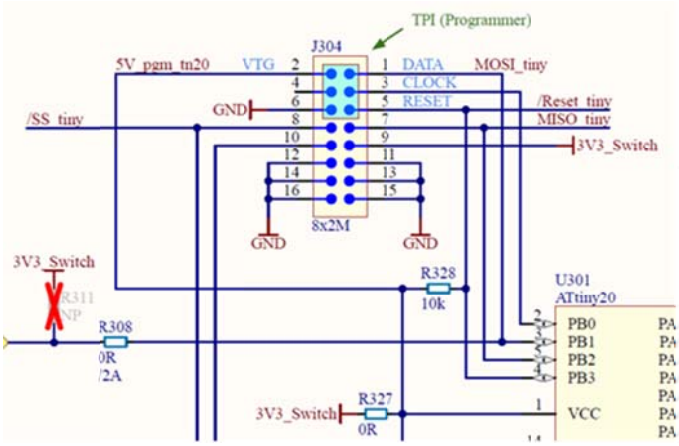


Abb. 71) Belegung des Tiny Programming Interface (TPI)

4.1.4 LEDs & Funktionstasten

Die dreifach LED Gruppe (**2**) D12 (grün), D9 (rot) und D11 (gelb) visualisiert den TAG Erkennungsstatus während eines Lesevorgangs. Folgende Möglichkeiten sind detektierbar:

- grüne LED (D12, linke LED in Abb. 68)
  TAG mit unterstütztem Format nach ISO-Standard detektiert und Speichergröße gültig.

- gelbe LED (D11, rechte LED in Abb. 68)
  TAG mit unterstütztem Format nach ISO-Standard detektiert, aber Signalstärke schwach. Keine Information über Speichergröße verfügbar.

- rote LED (D9, mittlere LED in Abb. 68)
  TAG erkannt, aber Format wird von der Reader Firmware nicht unterstützt.

Eine positive TAG Erkennung wird immer mit einer Tonausgabe durch softwaremäßige Ansteuerung von Beeper (**4**) unterstützt.

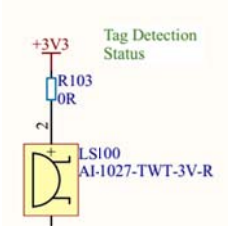


Abb. 72) Tonerzeugung mit Beeper

Die LED Kaskade (**6**) ist in zwei Hierarchien mit je drei LEDs aufgeteilt. Ihre Kodierung entspricht dem Schaltzustand der zurzeit aktiven Antennenposition, durch den 1:5 Multiplexer mit 25 Antennen in Variante A. Die aktuelle Position kann aus den Signalzuständen der Tabelle 10 abgeleitet werden.

Stufe 1	Stufe 2	Antenne Nr.
		1
		2
		3
		4
		5
		6
		7
		8
		9
		10
		11
		12
		13
		14
		15
		16
		17
		18
		19
		20
		21
		22
		23
		24
		25

*Tab. 10) Kodierungstabelle der Antennenpositionen mit Status LEDs (**6**)*

Die Taste (**1**) löst nach einmaliger Betätigung einen Master Reset mit Neustart der Elektronik aus. Dabei werden sowohl die Stromversorgung sowie aktive Datenschnittstellen unterbrochen. Der Reader befindet sich anschließend wieder im Ausgangszustand, d.h. Antenne eins ist ausgewählt und der automatische Hardware Suchmodus (AHS) aktiv. Eine Endgerätekommunikation benötigt demzufolge wieder eine erneute Verbindungsaufnahme.

Die Taste (**2**) stellt eine Sonderfunktionstaste dar. Sie ist nur im automatischen Software Suchmodus (ASS) aktiv, der mittels Softwarebefehl ausgelöst wurde. Eine Betätigung der Taste beendet hier den Suchmodus und stoppt die zyklische Tonausgabe, falls sich aktuell ein TAG im aktiven Antennenfeld befindet. Der softwaregesteuerte Suchmodus funktioniert demzufolge mit allen verfügbaren Antennen und nicht nur mit der standardmäßigen Antennenposition eins [**1**] im automatischen Hardware Suchmodus (AHS) nach einem Neustart.

4.1.5 Firmware Update

Zur Behebung von Programmfehlern und/oder zur Einführung neuer Funktionen sind von Zeit zurzeit Firmware Aktualisierungen für den Reader geplant, die vom Anwender auch selbst installiert werden können. Sie sind damit vergleichbar mit sogenannten BIOS Updates für PC und Laptop. Als Voraussetzung für einen erfolgreichen Update Prozess muss ein Windows Rechner mit entsprechend installierten USB-Treibern für den XTC-ID Reader vorhanden sein. Das Update Paket wird in Form einer ZIP-Datei zum Download oder auf Anfrage per E-Mail Versand zur Verfügung gestellt. Es enthält alle notwendigen Programmdateien, so dass keine weitere externe Software benötigt wird. Nach dem Entpacken einer solchen *FlashToolxxx.zip* Datei, vornehmlich in ein leeres Verzeichnis, sollten mindestens die vier Dateien *bossac.**exe**, flash.**bat**, readme.**txt*** und *XTC-ID_Reader_xxx.**bin*** vorliegen. Die Textdatei erhält Informationen zur aktuellen Versionshistorie und beschreibt die notwendigen Schritte zur Durchführung der Aktualisierung in englischer Sprache.

ACHTUNG

Es sollten keinerlei Veränderungen an den Dateinamen oder dem Verzeichnisinhalt vorgenommen werden. Die Aktualisierung muss ausschließlich über die Batchdatei **flash.bat** eingeleitet werden, um korrekte Programmparameter sicherzustellen. Während des Update Prozesses darf keine Unterbrechung der Stromversorgung oder der Datenkommunikation erfolgen, da dies den XTC-ID Reader in einen nicht mehr bootfähigen Zustand hinterlassen würde. Während der Aktualisierung erfolgen Statusmeldungen im Terminalfenster der Eingabeaufforderung. Das Update ist erst beendet wenn dort die Meldung **CPU reset** ausgegeben wird!

Nachfolgende Schritte werden empfohlen:

1. Den XTC-ID Reader über ein USB-Kabel mit einem PC verbinden.
2. Öffnen des Gerätemanagers unter Windows, aktuelle COM-Port Nummer abfragen (Abb. 69)
3. Zweimal schnell hintereinander (Doppelklick) die Reset Taste (**1**) am Reader drücken.
4. Durch Schritt drei ändert sich der zugewiesene COM-Port der USB Verbindung und der Reader ist nun im Upload Modus. Eine Aktualisierung der Gerätemanager Anzeige zeigt die neu zugeordnete COM-Port Nummer (Abb. 73).
5. In dem Verzeichnis der entpackten Update Dateien eine Eingabeaufforderung (Command-Shell mit cmd.exe) öffnen.
6. In der Eingabezeile (Command Prompt) die Batchdatei mit der neuen COM-Port Nummer als Übergabeparameter starten (**flash x** <Enter>).
7. Die Aktualisierung ist erst beendet, wenn als Ausgabetext CPU reset erscheint. Nach einem Neustart des Readers kann dieser nun mit der neuen Firmware an der vorherigen COM-Port Nummer (Schritt 2) betrieben werden. Es empfiehlt sich gleich eine Grundkonfiguration der Einstellungen durchzuführen (siehe Kap. 4.2). Ein Beispiel der kompletten Terminalausgaben während des Updates Prozesses ist in Anhang C zu finden.

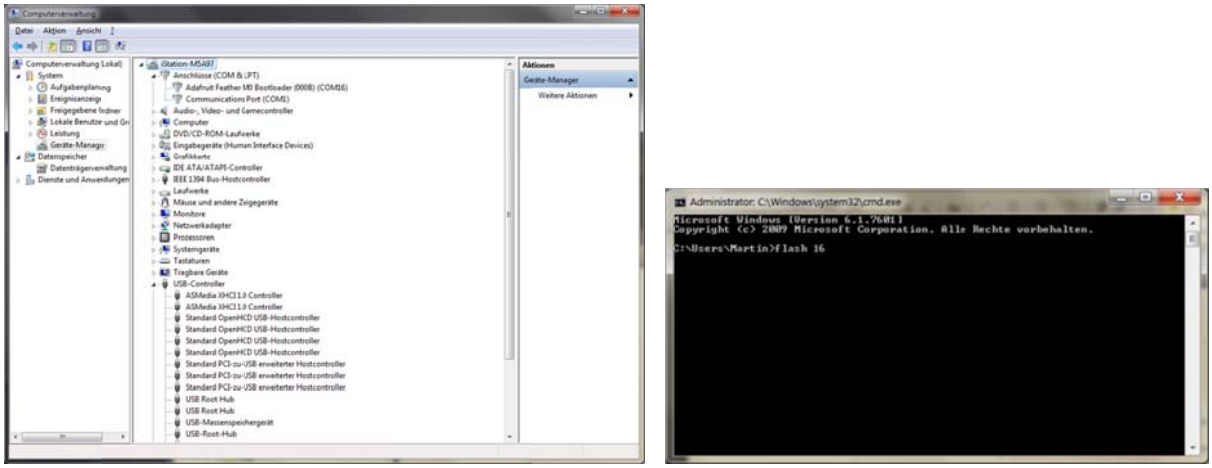


Abb. 73) Gerätemanager mit COM16 als Upload Port sowie zugehörige Befehlssequenz für Firmware Update

4.1.4 Antennen Tuner

Unser Stand-Alone Antennen-Tuner ist ein einzigartiges Werkzeug, das ein einfaches und kostengünstiges Tuning und Optimierung des Antennenabgleichs ermöglicht. Es ist insbesondere für den XTC-ID Reader der Variante B mit externen Antennen gedacht, da dieser die notwendigen Abgleich Kondensatoren (**8**) im Anpassungsnetzwerk schon direkt auf der Leiterplatte integriert hat. Prinzipiell ist der Tuner aber für jeden HF-kompatiblen RFID-Reader auf dem Markt geeignet. Nur mit Hilfe eines kleinen Schraubendrehers ermöglicht das batteriebetriebene Gerät dabei (Abb. 74), die Lesereichweite für RFID-Tags zu maximieren.

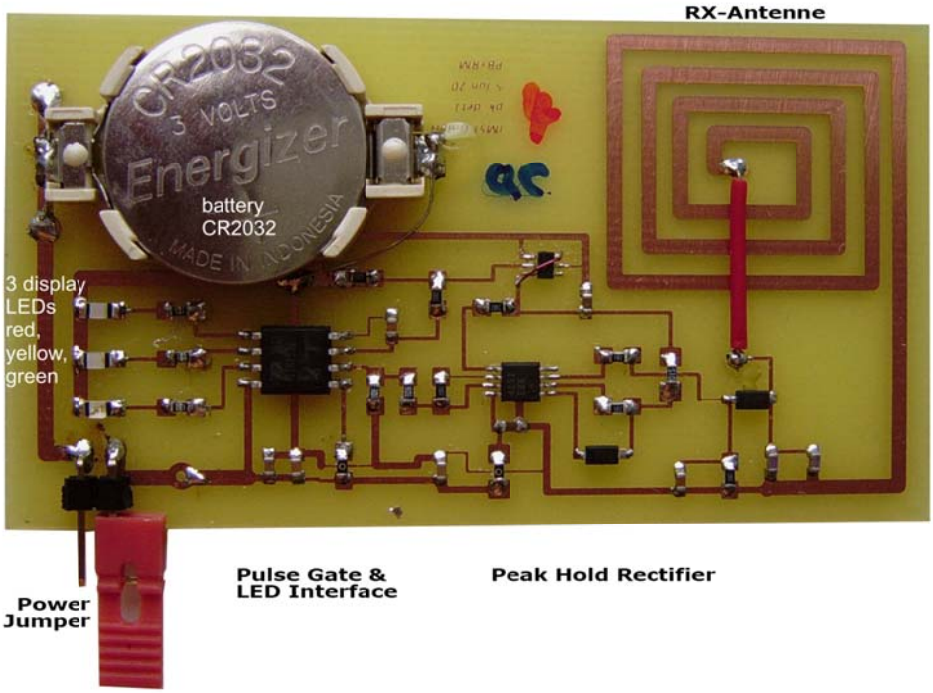


Abb. 74) Antennen Tuner Leiterplatte ohne Gehäuse

Das Funktionsprinzip beruht darauf, dass der XTC-ID Reader im automatischen Suchmodus (AHS) permanent, in Intervallen von etwa dreimal pro Sekunde (3Hz) nach TAGs im Antennenfeld scannt. Zu diesem Zweck werden kurze HF-Bursts bei 13,56 MHz vom Reader ausgesandt. Um die HF-Leistung dieser Bursts zu maximieren, ist die Resonanzkopplung beider beteiligten Antennen (Tuner & Reader) durch Feinjustierung am empfängerseitigen Antennenkondensator zu optimieren. Der Spitzenwertdetektor des Tuners protokolliert den Maximalwert der HF-Amplitude während dieser Bursts. Das Ergebnis wird direkt für jeden Burst auf der LED-Anzeige, in Form von drei Intensitätsstufen, mittels verschieden farbiger LEDs (rot, gelb grün) ausgegeben. Der relative Pegel der tatsächlich abgetasteten HF-Amplitude ergibt sich dabei als Kombination aller drei LED Anzeigen nach Tabelle 11. Bis auf die höchste und niedrigste Stufe wechseln die leuchtenden LEDs mit zunehmender Amplitude von Rot über Gelb nach Grün.

RF-Pegel (normalisiert)	ROTE LED	GELBE LED	GRÜNE LED
0			
1			
2			
3			
4			
5			
6			
7			

Tab. 11) Kodierungstabelle der RF-Amplituden nach LED Anzeige

Zur Abstimmung einzelner Reader-Antennen werden folgende Schritte empfohlen:

1. Die Batteriespannung am Tuner durch stecken der Drahtbrücke (Power Jumper) herstellen.
2. Externe Antenne mit dem Reader am gewünschten Eingang (EXT1 bis 6) verbinden. Den Reader einschalten, per Softwarebefehl die Antennenposition auswählen und automatischen Suchmodus (ASS) ausführen. Softwarekontrolle ist nur bei den Positionen 2 bis 6 notwendig, Antenne eins ist standardmäßig nach dem Einschalten aktiv (AHS).
3. Die Tuner Antenne im gewünschten Leseabstand von ca. 1 bis 3cm über die externe Antennenspule führen.
4. Stellen Sie die beiden Abstimmkondensatoren (**8**) an der Reader Antenne mit einem nicht leitenden Schraubendreher so ein, dass sich die HF-Amplitude auf der maximalen Skala nach Tabelle 11 befindet.
5. Eventuell den Vorgang ab Schritt 2 für weitere Antennenpositionen wiederholen.
6. Power-Jumper auf Parkposition stecken um die Batterie des Tuners zu schonen.
7. Anschließend die einwandfreie Funktion des Readers durch mehrmalige Lese- und Schreibvorgänge auf allen optimierten Antennenpositionen überprüfen.

4.2 Software Befehlssatz

Die notwendige USB-Treiberinstallation sowie die Lage der USB- und LAN-Schnittstelle wurde bereits in Kapitel 4.1.2 beschrieben. Für einen ersten Überblick des Befehlssatz sowie zur Konfiguration des Readers während der Erstinbetriebnahme, empfiehlt sich zunächst die Kommunikation mittels USB-Kabel. Hierzu wird nur ein Terminalprogramm benötigt welches eine serielle Datenkommunikation unterstützt. Hierfür eignet sich besonders das Freeware Programm „CoolTerm“[18], welches für Windows, macOS und Linux Betriebssysteme sowie als Raspberry Pi Version zur Verfügung steht, allerdings nur die serielle Kommunikation unterstützt (Abb. 75). Ein weiteres geeignetes Terminalprogramm ist die Open-Source Software „PuTTY“[19] die zusätzlich noch eine TCP/IP Schnittstelle mit Telnet Protokoll zur Verfügung stellt. Der XTC-ID Reader läuft automatisch (auto-sense) mit seriellen Datenübertragungsraten von 9600, 19200 oder 115200 Baud, acht Datenbits, keiner Parität und einem Stoppbit (z.B. 115200, 8, n, 1).

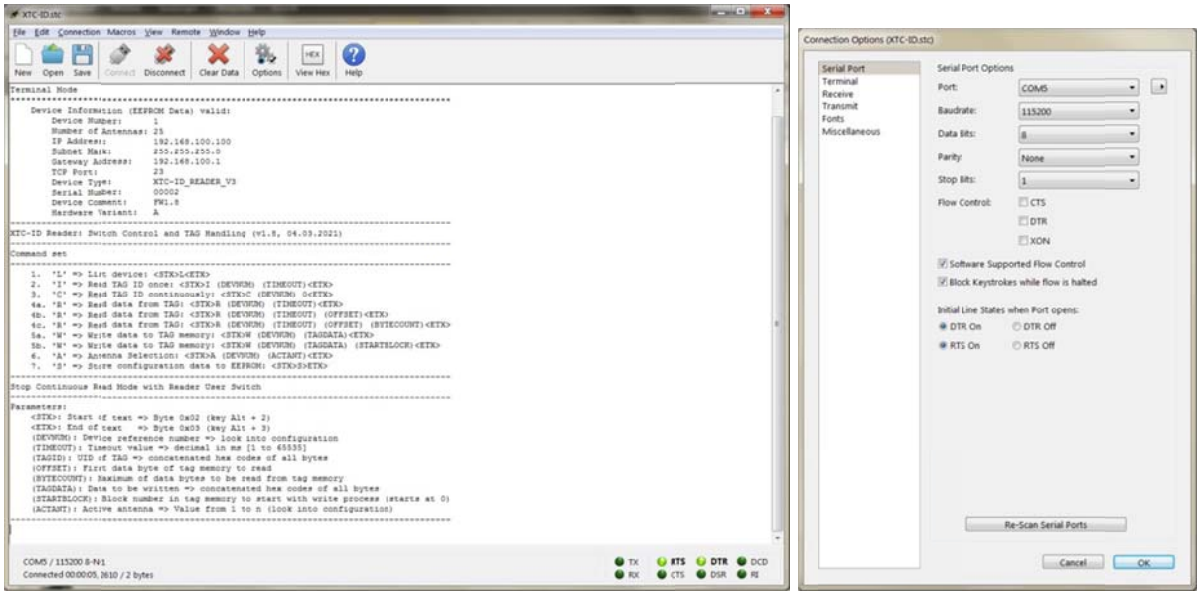


Abb. 75) CoolTerm[18] Terminalfenster mit entsprechenden Einstellungsparametern

Nach dem ersten Verbindungsaufbau und dem Empfang eines beliebigen Zeichens, antwortet der XTC-ID Reader durch Ausgabe des aktuellen Parametersatzes sowie einer Liste der verfügbaren Befehle samt Eingabesyntax. Jeder Befehl startet mit dem Steuerzeichen <STX> (0×02h „Start of Text“), welches auf Tastaturen mit deutschem Layout über die Tastenkombination Strg + B oder alternativ über Alt + 0 + 2 eingegeben werden kann. Analog wird der Befehl mit dem Steuerzeichen <ETX> (0×03h „End of Text“) abgeschlossen und direkt gesendet. Eine Betätigung der Enter Taste ist dabei nicht erforderlich. Hierzu können die Tastenkombinationen Strg + C oder alternativ Alt + 0 + 3 verwendet werden. Die eigentlichen Befehle bestehen aus reinen ASCII-Textzeichen, wobei Parameter durch Leerzeichen getrennt werden müssen. In der standardmäßigen Firmware ist die Datenkommunikation unverschlüsselt und eine Ein- oder Ausgabe erfolgt im hexadezimalen Format.

4.2.1 Reader Konfiguration

Nach dem Start des Terminalprogramms und herstellen einer Verbindung erfolgt zunächst die Ausgabe der aktuellen Konfigurationsparameter des angeschlossenen Readers über den Befehl ***L**ist device* (0x02 0x4C 0x03 ≡ <STX>L<ETX>). Eine Antwort ähnlich der folgenden wird zurückgegeben, wenn das Gerät ordnungsgemäß verbunden ist.

```
DEVNUM=1 ANT=25 IP=0.0.0.0 GW=0.0.0.0 NETMASK=255.255.0.0 PORT=23
DEVTYPE=XTC-ID_READER_V3 SERIALNUM=00004 DEVCOMMENT=FW1.8 VAR=A
```

Die Ausgabe gibt auch die Originalwerte nach einem Firmwareupdate wieder. Um Tippfehler zu vermeiden, empfiehlt es sich den Ausgabetext in die Zwischenablage zu kopieren und in einem separaten Texteditor entsprechend zu bearbeiten. Anschließend braucht der modifizierte Textstring nur einfach in das Terminalfenster zurück kopiert werden.

PARAMETER	WERT	BESCHREIBUNG
DEVNUM	1	Geräte Nummer im Netzwerk (def. 1)
ANT	6 oder 25	Anzahl an selektierbaren Antennen (def. 25)
IP	192.168.2.100	IP Nummer im Punktformat (def. 0.0.0.0)
GW	192.168.2.1	IP Nummer des Gateway/Routers (def. 0.0.0.0)
NETMASK	255.255.255.0	Netzwerkmaske (def. 255.255.0.0)
PORT	23	TCP/IP Port (def. Telnet Port 23)
DEVTYPE	XTC-ID_READER_V3	Gerätetyp mit Versionsnummer [optional]
SERIALNUM	00004	interne Seriennummer [optional] (def. 00000)
DEVCOMMENT	FW1.8	Geräteinfo mit Firmware Version [optional]
VAR	A oder B	Geräte Variante [A=25] [B=6] Antennen

Tab. 12) Parameterdefinition im Konfigurationsmenü

Eine Beschreibung der Parameter ist in oben stehender Tabelle 12 aufgelistet. Die drei orangefarbig hervorgehobenen Zeilen sollten nach einem Firmwareupdate auf jedem Fall überprüft und entsprechend angepasst werden. Gleichzeitig empfiehlt sich auch direkt die Vergabe der blau unterlegten TCP/IP Parameter, um gegebenenfalls auf eine LAN-Kommunikation umsteigen zu können. Der XTC-ID Reader benötigt in der aktuellen Firmware Version 1.8 eine feste IP-Nummer und unterstützt bislang nicht das DHCP-Protokoll. Die Änderung der Konfiguration erfolgt über den Befehl **S**tore configuration parameter (0x02 0x53 [P1] [P2] … [P10] 0x03 ≡ <STX>S [P1] [P2] … [P10]<ETX>) unter Übergabe der mit Leerzeichen separierten 10 Parameter.

```
<STX>S DEVNUM=2 ANT=6 IP=192.168.2.100 GW=192.168.2.1
NETMASK=255.255.255.0 PORT=456 DEVTYPE=XTC-ID_READER_V3
SERIALNUM=00004 DEVCOMMENT=FW1.8 VAR=B<ETX>
```

ACHTUNG

Leerzeichen innerhalb eines Parametersatzes werden nicht unterstützt (z.B. DEVTYPE in Tab. 12).

4.2.2 Auflistung aller Befehle

ACHTUNG

Bei allen Befehlszeichen wird nicht zwischen Groß- und Kleinschreibung unterschieden! Zum Beispiel ist der Syntax für Store configuration **S**, identisch zu **s**.

1. List device(s)

   Gibt Informationen über den angeschlossenen XTC-ID Reader zurück.
   Eingabe erfolgt mit <STX>L<ETX> ≡ (0x02 0x4C 0x03). Die Rückgabe der Gerätenummer DEVNUM ist für alle weiteren Kommandos essentiell. Diese muss für alle Geräte im Netzwerk eindeutig vergeben werden. Die Bedeutung der anderen Parameter sind der Tabelle 12 zu entnehmen.

   <STX>L<ETX>
   ```
   DEVNUM=1 ANT=6 IP=0.0.0.0 GW=0.0.0.0 NETMASK=255.255.0.0
   PORT=23 DEVTYPE=XTC-ID_READER_V3 SERIALNUM=00004
   DEVCOMMENT=FW1.8 VAR=B
   ```

2. Read TAG ID once

   Gibt einmalig die TAG ID sowie den maximal verfügbaren Speicherbereich in Bytes unter Berücksichtigung einer Zeitüberschreitung (Timeout), für einen TAG im HF-Feld der aktiven Antenne zurück.
   Eingabe erfolgt beispielsweise mit <STX>I 1 1000<ETX>. Lese die TAG ID im aktiven Antennenfeld auf Reader 1 mit einem Timeout Wert von 1000mS (eine Sekunde) aus.

   <STX>I 1 1000<ETX>
   ```
   908 1 0 e0040150bd61e7f4 112
   ```

PARAMETER	WERT	BESCHREIBUNG
EVENT	908	Event-Nachricht: "TAG ID vom Reader"
DEVNUM	1	Geräte Nummer im Netzwerk
ERRORCODE	0	Bei einer Fehlernummer > 0, folgen zwei Text-zeichenfolgen mit Fehlerinfo.
TAGID	e0040150bd61e7f4	eindeutige TAG ID
TAGSIZE	112	TAG Speicher (maximale Anzahl Bytes die geschrieben werden können.

3. Read TAG ID **C**ontinuously (ASS Mode)

   Gibt kontinuierlich die TAG ID sowie den maximal verfügbaren Speicherbereich in Bytes ohne Zeitüberschreitung (Timeout), für einen TAG im HF-Feld der aktiven Antenne zurück. Dieser Befehl entspricht dem automatischen Software Suchmodus (ASS). Dieser Befehl kann nur durch Betätigung der Funktionstaste (**3**) wieder verlassen werden (Kap. 4.1.4)!
   Eingabesyntax unter Eingabe der Gerätenummer und einem Nullwert für den Timeout mit:

```
<STX>C 1 0<ETX>
909 1 0 e0040150bd61e7f4 112 (28 x 4)
…
909 1 0 e0040150bd61e7f4 112 (28 x 4)
Continuous Mode stopped
```

PARAMETER	WERT	BESCHREIBUNG
EVENT	909	Event-Nachricht: "TAG ID vom Reader"
DEVNUM	1	Geräte Nummer im Netzwerk
ERRORCODE	0	Bei einer Fehlernummer > 0, folgen zwei Text-zeichenfolgen mit Fehlerinfo.
TAGID	e0040150bd61e7f4	eindeutige TAG ID
TAGSIZE	112	TAG Speicher (maximale Anzahl Bytes die geschrieben werden können.
MEMORY BLOCK	28 × 4	Speicherorganisation, z.B. 28 Blöcke mit je 4 Byte
STOP	Continuous Mode stopped	Funktionstaste (**3**) gedrückt, ASS Modus beendet

4. **R**ead Data from TAG

   Liest den kompletten TAG Speicher, unter Berücksichtigung einer Zeitüberschreitung (Timeout) in Form einer hexadezimalen Ausgabe aus. Dieser Befehl ist mit zwei weiteren optionalen Parametern ausgestattet, die auch einen sequentiellen Speicherblock Zugriff ermöglichen.
   Eingabe erfolgt beispielsweise mit <STX>R 1 1000<ETX>. Lese den kompletten TAG Speicher im aktiven Antennenfeld auf Reader 1 mit einem Timeout Wert von 1000mS (eine Sekunde) aus. In der unten stehenden Beispielausgabe ist der TAG Speicher ohne Daten sowie die TAG ID Bytefolge (low Byte / high Byte) vertauscht.

```
<STX>R 1 1000<ETX>
906 1 0 f4e761bd500104e0
00000000000000000000000000000000000000…
```

PARAMETER	WERT	BESCHREIBUNG
EVENT	906	Event-Nachricht: "TAG Daten vom Reader"
DEVNUM	1	Geräte Nummer im Netzwerk
ERRORCODE	0	Bei einer Fehlernummer > 0, folgen zwei Text-zeichenfolgen mit Fehlerinfo.
TAGID	f4e761bd500104e0	eindeutige TAG ID
TAGDATA	112 × 00…00	TAG Daten 112 Bytes (Anzahl der ausgelesenen Bytes entsprechen TAGSIZE)

OFFSET Parameter
Der optionale Byte Offset Parameter, definiert die Anzahl an Bytes die vom Datensatzanfang übersprungen werden, bevor der Lesezugriff beginnt. D.h. es bezeichnet die Speicherposition (Sprungmarke) ab der der Speicher bis zum Ende ausgelesen wird. Bytezählung beginnt bei null bis zur maximalen Byteanzahl (TAGSIZE – 1). Im untenstehenden Beispiel wird demzufolge nur das letzte Byte (112) ausgelesen.

```
<STX>R 1 1000 111<ETX>
906 1 0 f4e761bd500104e0
00
```

BYTECOUNT Parameter
Der optionale Byte BYTECOUNT Parameter, definiert in Kombination mit dem OFFSET Parameter die Anzahl an Bytes die von der Offset Sprungmarke an insgesamt ausgelesen werden. Im untenstehenden Beispiel werden demnach nur die beiden letzten Bytes (111 & 112) ausgelesen.

```
<STX>R 1 1000 110 2<ETX>
906 1 0 f4e761bd500104e0
0000
```

5. Write Data to TAG Memory

Schreibt einen Datensatz in Form einer hexadezimaler Zeichenfolge in den TAG Speicher ab einer definierten Block Nummer, ohne Berücksichtigung einer Zeitüberschreitung (Timeout). Dieser Befehl ist infolge der Blockangabe für einen sequentiellen blockweisen Schreibzugriff geeignet.
Eingabe erfolgt beispielsweise mit <STX>W 1 48656C6C6F20576F726C6421 0<ETX>. Schreibe den Text *Hello World!* in den TAG Speicher im aktiven Antennenfeld auf Reader 1 mit einem Timeout Wert von 1000mS (eine Sekunde). Der Schreibzugriff erfolgt ab Block null (Speicheranfang), wobei bestehende Daten überschrieben werden.

```
<STX>W 1 48656C6C6F20576F726C642 0<ETX>
907 1 0 f4e761bd500104e0 112
```

PARAMETER	WERT	BESCHREIBUNG
EVENT	907	Event-Nachricht: "Daten in TAG geschrieben"
DEVNUM	1	Geräte Nummer im Netzwerk
ERRORCODE	0	Bei einer Fehlernummer > 0, folgen zwei Text-zeichenfolgen mit Fehlerinfo.
TAGID	f4e761bd500104e0	eindeutige TAG ID
TAGSIZE	112	TAG Speicher (maximale Anzahl Bytes die insgesamt geschrieben werden können.

Ein nachfolgendes Auslesen des gerade beschriebenen TAGs, bestätigt den erfolgreichen Schreibvorgang:

```
<STX>R 1 1000<ETX>
906 1 0 f4e761bd500104e0
48656c6c6f20576f726c6421000000000000000…
```

6. Antenna Selection

Dieser Befehl wählt eine aktive Antennenposition unter den zur Verfügung stehenden Antennen für weitere Schreib- und Leseaktionen aus. Je nach Variante ist die maximale Anzahl unterschiedlich. In Variante A stehen 25 fest integrierte Antennen zur Verfügung, während die Variante B mit bis zu sechs externen Antennen ausgerüstet werden kann. Die aktuelle Anzahl kann in der Reader Konfiguration (Kap. 4.1.1) festgelegt und mit dem List device Befehl ausgelesen werden.
Zur Auswahl einer aktiven Antenne, beispielsweise auf Gerät 1 in Position 4 lautet der entsprechende Befehl zum Umschalten <STX>A 1 4<ETX>.

<STX>A 1 4<ETX>
Variant A Set
91B 1 0 4

PARAMETER	WERT	BESCHREIBUNG
EVENT	91B	Event-Nachricht: "Antenne ausgewählt"
DEVNUM	1	Geräte Nummer im Netzwerk
ERRORCODE	0	Bei einer Fehlernummer > 0, folgen zwei Text-zeichenfolgen mit Fehlerinfo.
ACTANT	4	neue aktive Antennenposition

4.2.3 Ereignis & Fehler Nachrichten

Alle nach einer Befehlseingabe vom Reader quittierten Rückmeldungen, starten mit einer dreistelligen Ereignis (Event) Nummer, als ersten Parameter im Rückgabetext. Solche Ereignis-meldungen sind asynchron und können zu einem beliebigen Zeitpunkt, spätestens nach Ablauf der Zeitüberschreitungsschwelle empfangen werden. Eine Liste aller definierten Ereignisse sind in Tabelle 13 aufgeführt.

EVENT	DESCRIPTION
900	Befehl fehlerhaft oder nicht unterstützt
906	TAG Daten ausgelesen (READ Event)
907	Daten in TAG geschrieben (WRITE Event)
908	TAG ID & Speichergröße ausgelesen (READ ID Event)
909	TAG ID, Speichergröße, Blockanzahl empfangen (continuous read mode)
91A	Reader Konfiguration abgeschlossen (STORE Event)
91B	Reader Antenne ausgewählt (ACTANT Event)

Tab. 13) Ereignisnummern und ihre Bedeutung

In Tabelle 14 sind die Fehlercodes aufgelistet, die möglicherweise erhalten werden, obwohl ein zulässiger Befehl mit einer korrekten Anzahl von Parametern empfangen wurde.

COMMAND	ERROR CODE	ERROR MESSAGE	CAUSE
Read Tag	-1	BUSY	device init in progress
	-2	Offset out of range (-1...8191)	invalid parameter
	-3	Byte count out of range (-1...8191)	invalid parameter
	-4	No Antenna selected	
	-20…-999	BUSY	device already busy
	-1000	Invalid device	device number out of range
	-1002	Command not supported	invalid parameter

COMMAND	ERROR CODE	ERROR MESSAGE	CAUSE
Read Tag **I**D	-1	BUSY	device init in progress
	-4	No Antenna selected	
	-20…-999	BUSY	device already busy
	-1000	Invalid device	device number out of range
	-1002	Command not supported	invalid parameter

COMMAND	ERROR CODE	ERROR MESSAGE	CAUSE
Write Tag	-1	BUSY	device init in progress
	-2	Parameter "TAGDATA" contains invalid characters	
	-4	No Antenna selected	
	-20…-999	BUSY	device already busy
	-1000	Invalid device	device number out of range
	-1002	Command not supported	invalid parameter

COMMAND	ERROR CODE	ERROR MESSAGE	CAUSE
Set **A**ntenna	-1	BUSY	device init in progress
	-2	Reader does not support antenna selection	
	-3	Invalid antenna (VAR A 1...25, VAR B 1...6 external)	
	-4	Invalid antenna, reader supports 1…[N]	
	-20…-999	BUSY	device already busy
	-1000	Invalid device	device number out of range
	-1002	Command not supported	invalid parameter

Tab. 14) Fehlercodes und ihre Bedeutung

Literaturverzeichnis

1. **NXP Semiconductors.** Product data sheet S2S2602. *ICODE SLIX2.* v. 4.1, Juli 25, 2017. www.nxp.com.

2. **ISO/IEC JTC 1/SC 17.** Cards and security devices for personal identification. [Online] https://www.iso.org/committee/45144.html.

3. **Paplewski, Dr. Martin and Schulze, Siegfried.** *Chemisch inerter RFID Transponder zur Objektkennzeichnung bei hohen Temperaturen. DE102009033900A1* Januar 27, 2011. Patent.

4. **NXP Semiconductors.** MIFARE product and handling of UIDs. [Online] July 5, 2018. https://www.nxp.com/docs/en/application-note/AN10927.pdf. Application note AN10927.

5. **IMST GmbH, Dr. Uhlig, Peter.** *LTCC Materials and Process in a nutshell.* 2017. Präsentation.

6. **Dr.-Ing. Luniak, Marco.** *Institutskolloquium Aufbau- und Verbindungstechnik.* s.l. : Institut für Elektronik-Technologie der TU Dresden, 2004.

7. **Dr. Rebenklau, Lars;.** *Konzepte zur Unterdrückung des Sinterschrumpfes.* s.l. : FhG IKTS, 2007. Zero-Shrink-Studie TU Dresden.

8. **Schwanke, Dieter.** Neue Wege zur Erhöhung von Integrationsdichte und Mehrfachnutzen hochintegrierter keramischer Mehrlagenschaltungen. *BayFOR.* [Online] II-4 S.121 (2001). https://www.bayfor.org/fileadmin/user_upload/forschungsverbuende/forkeram/BayFOR-forkeram-abschlussbericht2001-teil3.pdf.

9. **Jones, William, et al., et al.** Chemical, structural and mechanical properties of the LTCC tapes. *ResearchGate.* [Online] 2000. https://www.researchgate.net/publication/228812066_Chemical_structural_and_mechanical_properties_of_the_LTCC_tapes.

10. **Chaudhary, A., et al., et al.** A Novel Fabrication Technique of Cylindrical Ion Traps using Low Temperature Co-fired Ceramic Tapes. *NSTI-Nanotech.* 2004, Vols. Vol. 1, 371-373.

11. **Fujitsu Semiconductor Memory Solution Ltd.** Fujitsu starts mass-production of 4Mbit FRAM with 125°C operation. [Online] July 2021. https://www.fujitsu.com/jp/group/fsm/en/about/resources/news/press-releases/2021/0706.html.

12. **Infineon.** F-RAM (Ferroelectric RAM). [Online] 2021. https://www.infineon.com/cms/en/product/memories/f-ram-ferroelectric-ram.

13. **Doering, Robert and Nishi, Yoshio.** Handbook of Semiconductor - Manufacturing Technology. 2nd. Edition. ISBN 9781420017663 : CRC Press, 2008, Kap. 32/ S. 14.

14. **Röhrich, Tobias.** *Technical Information.* s.l. : nano-join GmbH, 09/2018. Company confidental.

15. *RFID Tag Failure After Thermal Overstress.* **Ozturk, Emre, et al., et al.** [ed.] University of Twente. 2019. IEEE International Integrated Reliability Workshop (IIRW). p. 4. DOI: 10.1109/IIRW47491.2019.8989885.

16. **NXP Semiconductors.** PN7150 - High performance NFC controller with integrated firmware. *Product data sheet 317439.* v.3.9, August 28., 2019. www.nxp.com.

17. **Adafruit Windows Drivers.** GitHub-adafruit. [Online] v.2.5.0.0, November 12, 2021. https://github.com/adafruit/Adafruit_Windows_Drivers/releases.

18. **Roger Meier's Freeware.** CoolTerm (serial port terminal application). [Online] v.1.9.1, November 11, 2021. http://freeware.the-meiers.org.

19. **Simon Tatham.** PuTTY: a free SSH and Telnet client. [Online] Juli 17, 2021. https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html.

Anhang A

ISO/IEC JTC1/SC17 STANDING DOCUMENT 5 (March 2018)
Register of IC manufacturers[2)]

UID - Identifier	Company	Country
0x**01**	Motorola	United Kingdom
0x**02**	STMicroelectronics SA	France
0x**03**	Hitachi, Ltd	Japan
0x**04**	NXP Semiconductors B.V.	Netherland
0x**05**	Infineon Technologies AG	Germany
0x**06**	Cylink	USA
0x**07**	Texas Instrument	France
0x**08**	Fujitsu Limited	Japan
0x**09**	Matsushita Electronics Corporation	Japan
0x**0A**	NEC	Japan
0x**0B**	Oki Electric Industry Co. Ltd	Japan
0x**0C**	Toshiba Corp.	Japan
0x**0D**	Mitsubishi Electric Corp.	Japan
0x**0E**	Samsung Electronics Co. Ltd	Korea
0x**0F**	Hynix	Korea
0x**10**	LG-Semiconductors Co. Ltd	Korea
0x**11**	Emosyn-EM Microelectronics	USA
0x**12**	INSIDE Technology	France
0x**13**	ORGA Kartensysteme GmbH	Germany
0x**14**	SHARP Corporation	Japan
0x**15**	ATMEL	France
0x**16**	EM Microelectronic-Marin SA	Switzerland
0x**17**	SMARTRAC TECHNOLOGY GmbH	Germany
0x**18**	ZMD AG	Germany
0x**19**	XICOR, Inc.	USA
0x**1A**	Sony Corporation	Japan
0x**1B**	Malaysia Microelectronic Solutions Sdn. Bhd	Malaysia
0x**1C**	Emosyn	USA
0x**1D**	Shanghai Fudan Microelectronics Co. Ltd.	P.R. China
0x**1E**	Magellan Technology Pty Limited	Australia
0x**1F**	Melexis NV BO	Switzerland
0x**20**	Renesas Technology Corp.	Japan
0x**21**	TAGSYS	France
0x**22**	Transcore	USA
0x**23**	Shanghai belling Corp., Ltd.	P.R. China
0x**24**	Masktech Germany GmbH	Germany
0x**25**	Innovision Research and Technology Plc	United Kingdom
0x**26**	Hitachi ULSI Systems Co., Ltd.	Japan
0x**27**	Yubico AB	Sweden

UID - Identifier	Company	Country
0x**28**	Ricoh	Japan
0x**29**	ASK	France
0x**2A**	Unicore Microsystems, LLC	Russia
0x**2B**	Dallas Semiconductor/Maxim	USA
0x**2C**	Impinj, Inc.	USA
0x**2D**	RightPlug Alliance	USA
0x**2E**	Broadcom Corporation	USA
0x**2F**	MStar Semiconductor, Inc	Taiwan, ROC
0x**30**	BeeDar Technology Inc.	USA
0x**31**	RFIDsec	Denmark
0x**32**	Schweizer Electronic AG	Germany
0x**33**	AMIC Technology Corp	Taiwan, ROC
0x**34**	Mikron JSC	Russia
0x**35**	Fraunhofer Institute for Photonic Microsystems	Germany
0x**36**	IDS Microchip AG	Switzerland
0x**37**	Kovio	USA
0x**38**	HMT Microelectronic Ltd.	Switzerland
0x**39**	Silicon Craft Technology	Thailand
0x**3A**	Advanced Film Device Inc.	Japan
0x**3B**	Nitecrest Ltd.	United Kingdom
0x**3C**	Verayo Inc.	USA
0x**3D**	HID Global	USA
0x**3E**	Productivity Engineering GmbH	Germany
0x**3F**	Austriamicrosystems AG (reserved)	Austria
0x**40**	Gemalto SA	France
0x**41**	Renesas Electronics Corporation	Japan
0x**42**	3Alogics Inc.	Korea
0x**43**	Top TroniQ Asia Limited	Hong Kong
0x**44**	Gentag Inc. (USA)	USA
0x**45**	Invengo Information Technology Co.Ltd.	China
0x**46**	Guangzhou Sysur Microelectronics, Inc.	China
0x**47**	CEITEC S.A.	Brazil
0x**48**	Shanghai Quanray Electronics Co. Ltd.	China
0x**49**	MediaTek Inc.	Taiwan
0x**4A**	Angstrem PJSC	Russia
0x**4B**	Celisic Semiconductor (Hong Kong) Limited	China
0x**4C**	LEGIC Identsystems AG	Switzerland
0x**4D**	Balluff GmbH	Germany
0x**4E**	Oberthur Technologies	France
0x**4F**	Silterra Malaysia Sdn. Bhd.	Malaysia
0x**50**	DELTA Danish Electronics, Light & Acoustics	Denmark
0x**51**	Giesecke & Devrient GmbH	Germany
0x**52**	Shenzhen China Vision Microelectronics Co., Ltd.	China

UID - Identifier	Company	Country
0x**53**	Shanghai Feiju Microelectronics Co. Ltd.	China
0x**54**	Intel Corporation	USA
0x**55**	Microsensys GmbH	Germany
0x**56**	Sonix Technology Co., Ltd.	Taiwan
0x**57**	Qualcomm Technologies Inc.	USA
0x**58**	Realtek Semiconductor Corp.	Taiwan
0x**59**	Freevision Technologies Co. Ltd.	China
0x**5A**	Giantec Semiconductor Inc.	China
0x**5B**	JSC Angstrem-T	Russia
0x**5C**	STARCHIP	France
0x**5D**	SPIRTECH	France
0x**5E**	GANTNER Electronic GmbH	Austria
0x**5F**	Nordic Semiconductor	Norway
0x**60**	Verisiti Inc.	USA
0x**61**	Wearlinks Technology Inc.	China
0x**62**	Userstar Information Systems Co., Ltd.	Taiwan
0x**63**	Pragmatic Printing Ltd.	United Kingdom
0x**64**	Associação do Laboratório de Sistemas Integráveis Tecnológico – LSI-TEC	Brazil
0x**65**	Tendyron Corporation	China
0x**66**	MUTO Smart Co., Ltd.	Korea
0x**67**	ON Semiconductor	USA
0x**68**	TÜBİTAK BİLGEM	Turkey
0x**69**	Huada Semiconductor Co., Ltd.	China
0x**6A**	SEVENEY	France
0x**6B**	ISSM	France
0x**6C**	Wisesec Ltd.	Israel
0x**7E**	Holtek	Taiwan

Anhang B

Datenblatt und Produktinformation

*xt*ID *C33HF / C25HF / C10HF Transponder*

1. Produktbezeichnung/-beschreibung

(November 2021 V11)

Die ***xt*ID CHF** Transponder verbinden eine maximale Industriebeständigkeit mit der absoluten Freiheit hinsichtlich Größe, Technologie und Anbringungsart. Grundmaterial ist ein vollkommen inertes und chemikalienbeständiges Keramiksubstrat. Seine erweiterte Temperaturbeständigkeit ermöglicht dabei Applikationen in Einsatzbereichen von -190°C bis +400°C. Der Transponder kann sowohl mit dem Smartphone/Tablet als auch mit einem HF Reader gelesen und beschrieben werden. Eine Zertifizierung nach ATEX und IECEx ist in Vorbereitung.

Typische Anwendungen:

- chemische Industrie, Laboratorien
- Medizintechnik, Pharmaindustrie
- Luft- & Raumfahrttechnik
- Batteriemodulfertigung
- Sondermülldeponien

xtID C33HF

C25HF

C10HF

2. Produktaufbau

RFID Chip

▪ ISO-Norm	ISO/IEC15695
▪ Typ	ICODE SLIX2 (NXP Semiconductors) SL2S2602 / Product data sheet ICODE SLIX2 Rev. 4.1 — 25 July 2017 (276341)
▪ RFID System Frequenz	13,56 MHz, HF-Band
▪ Speicher	User Memory 2560 bits (80 Blöcke a 4 Bytes)
▪ Schreibzyklen	min. 100.000 pro Lebenszeit
▪ Datenerhalt	> 20 Jahre (bei T < 350°C)

RFID Transponder

▪ Format	quadratisch
▪ Abmessungen	33×33 mm (CHF33), 25×25 mm (CHF25), 10×10 mm (CHF10)
▪ Dicke	0,51 – 0,56 mm

RFID Transponder (Fortsetzung)

▪ Montageloch	2 Stück 3,5 mm (M3), außer C10HF
▪ Substratmaterial	low temperature co-fired ceramic (LTCC) keramisches Mischoxid (Al_2O_3/SiO_2) Farbe lichtblau, RAL 5012 unbedruckt, 4-Farben Digitaldruck auf Anfrage möglich
▪ Antennenmaterial	Gold/Palladium (Au/Pd) Legierung
▪ Verkapselungsmaterial	Bornitrid (BN) mit anorganischem Binder (CaO/SiO_2)

Beständigkeiten

▪ Max. Betriebstemperatur	-190°C bis +156°C
▪ Max. Lagertemperatur	-190°C bis +400°C
▪ Maximaltemperatur	Erfolgreicher Test bei +450°C für 3 h
▪ Luftfeuchtigkeit	0 % – 100 %RH
▪ UV-Strahlung	Erfolgreicher Test nach DIN EN ISO 4892-2
▪ Witterung	Erfolgreicher Test nach Renault D27 1911 (02/95)
▪ Klima	Erfolgreicher Test nach Renault 1309 (09/81)
▪ Chemische Beständigkeit	Sehr gute Beständigkeit nach 120h Eintauchen in Wasser, Salzwasser, Säure, Laugen, Ethylenglycol, aromatische und Halogen-Kohlenwasserstoffe, polare Lösungsmittel (Alkohole, Ester und Ketone), Dauereinwirkung von heißem Wasser.
▪ Bruch-/Schlagbeständigkeit	empfindlich gegen Schlageinwirkung und Scherkräfte
▪ Formbeständigkeit	unbegrenzt schrumpffrei

Normen/Zulassungen (ab Produktionsjahr 2022)*

- Erfüllt REACH-Verordnung (EG) 1907/2006
- Erfüllt RoHS-Richtlinie 2011/65/EU
- Erfüllt CE-Richtlinie
- Blei- und Quecksilberfrei (EU 2017/852)

*) vorherige Chargen enthalten bis zu 8 % Beimengungen von Bleioxid (PbO) im Keramiksubstrat

Anhang C

Terminalausgabe beim Firmware Update

```
>D:\FlashTool 1.8.0\FlashTool>flash 16

D:\FlashTool 1.8.0\FlashTool>bossac.exe --port=COM16 -l15
Atmel SMART device 0x10010005 found
Lock region 15
D:\FlashTool 1.8.0\FlashTool>bossac.exe --port=COM16 -i
Atmel SMART device 0x10010005 found
Device       : ATSAMD21G18A
Chip ID      : 10010005
Version      : v2.0 [Arduino:XYZ] Mar  5 2016 17:46:52
Address      : 8192
Pages        : 3968
Page Size    : 64 bytes
Total Size   : 248KB
Planes       : 1
Lock Regions : 16
Locked       : 15
Security     : false
Boot Flash   : true
BOD          : true
BOR          : true
Arduino      : FAST_CHIP_ERASE
Arduino      : FAST_MULTI_PAGE_WRITE
Arduino      : CAN_CHECKSUM_MEMORY_BUFFER
D:\FlashTool 1.8.0\FlashTool>bossac.exe --port=COM16 -d -e -w -v XTC-ID
_Reader_v1_8_2021_03_04.bin
Set binary mode
readWord(addr=0)=0x20007ffc
readWord(addr=0xe000ed00)=0x410cc601
readWord(addr=0x41002018)=0x10010305
version()=v2.0 [Arduino:XYZ] Mar  5 2016 17:46:52
chipId=0x10010005
Connected at 921600 baud
readWord(addr=0)=0x20007ffc
readWord(addr=0xe000ed00)=0x410cc601
readWord(addr=0x41002018)=0x10010305
Atmel SMART device 0x10010005 found
write(addr=0x20004000,size=0x34)
writeWord(addr=0x20004030,value=0x10)
writeWord(addr=0x20004020,value=0x20008000)
Erase flash
chipErase(addr=0x2000)
done in 0.827 seconds

Write 56376 bytes to flash (881 pages)
write(addr=0x20005000,size=0x1000)
writeBuffer(scr_addr=0x20005000, dst_addr=0x2000, size=0x1000)
[==                          ] 7% (64/881 pages)write(addr=0x20005000,size=0x1000)
writeBuffer(scr_addr=0x20005000, dst_addr=0x3000, size=0x1000)

[====                        ] 14% (128/881 pages)write(addr=0x20005000,size=0x1000)
writeBuffer(scr_addr=0x20005000, dst_addr=0x4000, size=0x1000)
[======                      ] 21% (192/881 pages)write(addr=0x20005000,size=0x1000)
writeBuffer(scr_addr=0x20005000, dst_addr=0x5000, size=0x1000)
[========                    ] 29% (256/881 pages)write(addr=0x20005000,size=0x1000)
writeBuffer(scr_addr=0x20005000, dst_addr=0x6000, size=0x1000)
[==========                  ] 36% (320/881 pages)write(addr=0x20005000,size=0x1000)
writeBuffer(scr_addr=0x20005000, dst_addr=0x7000, size=0x1000)
[============                ] 43% (384/881 pages)write(addr=0x20005000,size=0x1000)
writeBuffer(scr_addr=0x20005000, dst_addr=0x8000, size=0x1000)
[==============              ] 50% (448/881 pages)write(addr=0x20005000,size=0x1000)
writeBuffer(scr_addr=0x20005000, dst_addr=0x9000, size=0x1000)
[================            ] 58% (512/881 pages)write(addr=0x20005000,size=0x1000)
```

```
writeBuffer(scr_addr=0x20005000, dst_addr=0xa000, size=0x1000)
[==================           ] 65% (576/881 pages)write(addr=0x20005000,size=0x1000)
writeBuffer(scr_addr=0x20005000, dst_addr=0xb000, size=0x1000)
[====================         ] 72% (640/881 pages)write(addr=0x20005000,size=0x1000)
writeBuffer(scr_addr=0x20005000, dst_addr=0xc000, size=0x1000)
[======================       ] 79% (704/881 pages)write(addr=0x20005000,size=0x1000)
writeBuffer(scr_addr=0x20005000, dst_addr=0xd000, size=0x1000)
[========================     ] 87% (768/881 pages)write(addr=0x20005000,size=0x1000)
writeBuffer(scr_addr=0x20005000, dst_addr=0xe000, size=0x1000)
[==========================   ] 94% (832/881 pages)write(addr=0x20005000,size=0xc40)
writeBuffer(scr_addr=0x20005000, dst_addr=0xf000, size=0xc40)
[============================] 100% (881/881 pages)
done in 0.437 seconds

Verify 56376 bytes of flash with checksum.
checksumBuffer(start_addr=0x2000, size=0x1000) = 5257
checksumBuffer(start_addr=0x3000, size=0x1000) = c9a2
checksumBuffer(start_addr=0x4000, size=0x1000) = 28c0
checksumBuffer(start_addr=0x5000, size=0x1000) = 7c33
checksumBuffer(start_addr=0x6000, size=0x1000) = 8b8b
checksumBuffer(start_addr=0x7000, size=0x1000) = 406c
checksumBuffer(start_addr=0x8000, size=0x1000) = f826
checksumBuffer(start_addr=0x9000, size=0x1000) = 922f
checksumBuffer(start_addr=0xa000, size=0x1000) = 4243
checksumBuffer(start_addr=0xb000, size=0x1000) = b755
checksumBuffer(start_addr=0xc000, size=0x1000) = ec73
checksumBuffer(start_addr=0xd000, size=0x1000) = 146d
checksumBuffer(start_addr=0xe000, size=0x1000) = 71a4
checksumBuffer(start_addr=0xf000, size=0xc38) = d5a2
Verify successful
done in 0.094 seconds

D:\FlashTool 1.8.0\FlashTool>bossac.exe --port=COM16 -u

Atmel SMART device 0x10010005 found
Unlock all regions

D:\FlashTool 1.8.0\FlashTool>bossac.exe --port=COM16 -R

Atmel SMART device 0x10010005 found
CPU reset.
```

Anhang D

Terminalausgabe nach Neustart

```
Communication Mode: Serial

********************************************************************************
Terminal Mode
********************************************************************************
    Device Information (EEPROM Data) valid:
        Device Number:      1
        Number of Antennas: 6
        IP Address:         0.0.0.0
        Subnet Mask:        255.255.0.0
        Gateway Address:    0.0.0.0
        TCP Port:           23
        Device Type:        XTC-ID_READER_V3
        Serial Number:      00004
        Device Comment:     FW1.8
        Hardware Variant:   B
--------------------------------------------------------------------------------
XTC-ID Reader: Switch Control and TAG Handling (v1.8, 04.03.2021)
--------------------------------------------------------------------------------
Command set
--------------------------------------------------------------------------------
    1.  'L' => List device: <STX>L<ETX>
    2.  'I' => Read TAG ID once: <STX>I (DEVNUM) (TIMEOUT)<ETX>
    3.  'C' => Read TAG ID continuously: <STX>C (DEVNUM) 0<ETX>
    4a. 'R' => Read data from TAG: <STX>R (DEVNUM) (TIMEOUT)<ETX>
    4b. 'R' => Read data from TAG: <STX>R (DEVNUM) (TIMEOUT) (OFFSET)<ETX>
    4c. 'R' => Read data from TAG: <STX>R (DEVNUM) (TIMEOUT) (OFFSET) (BYTECOUNT)<ETX>
    5a. 'W' => Write data to TAG memory: <STX>W (DEVNUM) (TAGDATA)<ETX>
    5b. 'W' => Write data to TAG memory: <STX>W (DEVNUM) (TAGDATA) (STARTBLOCK)<ETX>
    6.  'A' => Antenna Selection: <STX>A (DEVNUM) (ACTANT)<ETX>
    7.  'S' => Store configuration data to EEPROM: <STX>S>ETX>
--------------------------------------------------------------------------------
Stop Continuous Read Mode with Reader User Switch
--------------------------------------------------------------------------------
Parameters:
    <STX>: Start of text => Byte 0x02 (key Alt + 2)
    <ETX>: End of text   => Byte 0x03 (key Alt + 3)
    (DEVNUM): Device reference number => look into configuration
    (TIMEOUT): Timeout value => decimal in ms [1 to 65535]
    (TAGID): UID of TAG => concatenated hex codes of all bytes
    (OFFSET): First data byte of tag memory to read
    (BYTECOUNT): Maximum of data bytes to be read from tag memory
    (TAGDATA): Data to be written => concatenated hex codes of all bytes
    (STARTBLOCK): Block number in tag memory to start with write process (starts at 0)
    (ACTANT): Active antenna => Value from 1 to n (look into configuration)
--------------------------------------------------------------------------------

Use S-Command with arguments of this pattern:
S  DEVNUM=1  ANT=25  IP=000.000.000.000  GW=000.000.000.000  NETMASK=000.000.000.000  PORT=80
DEVTYPE=XTC-ID_READER_V2 SERIALNUM=00001 DEVCOMMENT=FW1.7 VAR=A
The 10 entry fields are separated by blanks.
The command can also contain only one or a part of the configuration parameters.
Do not use blanks in the single entry fields!
--------------------------------------------------------------------------------
```