



**Smart Card
Alliance**



Mobile/NFC Security Fundamentals

NFC Forum Tags and Security Considerations

- **Smart Card Alliance and NFC Forum Webinar**
- **April 18, 2013**





**Smart Card
Alliance**

Introductions

- **Randy Vanderhoof**
- **Executive Director, Smart Card Alliance**

Mobile & NFC Council



- *Raise awareness and accelerate the adoption* of all applications using NFC
 - Access control, identity, loyalty, marketing, payments, peer-to-peer, promotion/coupons/offers, transit, ...
- *Accelerate the practical application of NFC*, providing a bridge between technology development/specifications and the applications that can deliver business benefits to industry stakeholders.



Today's Webinar Topics & Speakers



- **Introductions:** Randy Vanderhoof, Executive Director, Smart Card Alliance



- **NFC Forum Tags Types and Security Standards:** Tony Rosati, NFC Forum Security Work Group Chair & Blackberry



- **NFC Tag Uses, Applications and Sourcing Considerations:** Joe Tassone, Executive Vice President Technology & Product Management, Identive Group



- **Security for NFC Tag Applications:** Mike Zercher, Senior Applications Engineer, NXP Semiconductors



- **Tag Management and Market Perspective:** Rob Zivney, VP Marketing, Identification Technology Partners

- **Q&A:** Randy Vanderhoof, Smart Card Alliance



Smart Card
Alliance



NFC Forum Tag Types and Security Standards

- Tony Rosati
- Chair, NFC Forum Security Working Group
- Blackberry

NFC Forum Mission and Goals

- **The mission of the NFC Forum is to advance the use of NFC technology by:**
 - Developing standards-based specifications that ensure interoperability among devices and services
 - Encouraging the development of products using NFC Forum specifications
 - Educating the market globally about NFC technology
 - Ensuring that products claiming NFC capabilities comply with NFC Forum specifications
 - Promoting the NFC Forum N-Mark

We are Well into the Journey

Define and Stabilize Technology

Support Interoperability
Enhance Technology
Support Ecosystem

Refine Technology
Expand Ecosystem
Promote End User Usage

2008

2009

2010

2011

2012/13

Members – April 2013

SPONSOR MEMBERS

PRINCIPAL MEMBERS

Members – April 2013

ASSOCIATE MEMBERS

IMPLEMENTER MEMBERS

NONPROFIT MEMBERS

NFC - How Does It Work?

3 Communication Modes

Connect the world of apps with the physical world:

Apps jump into the world and touch people, objects and other apps.

Connect devices through physical proximity:

A magical connection of devices by simply touching them. A true device “hand shake”.

Interactive wallet:

Incorporates the use of a secure element to allow your phone to act like an “interactive card” for payment, transportation, ID and physical access

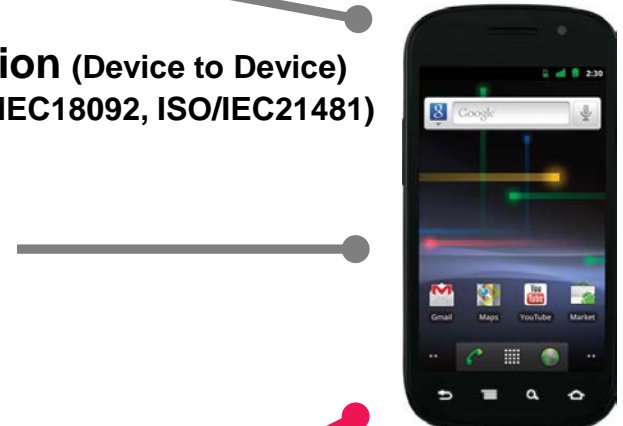
Tag/Card Reader/Writer (Terminal)

Multi-standard (ISO/IEC14443, JIS X 6319-4/Felica, ISO/IEC15693)



P2P Communication (Device to Device)

NFCIP-1, NFCIP-2 (ISO/IEC18092, ISO/IEC21481)



Card Emulation (Secure Element)

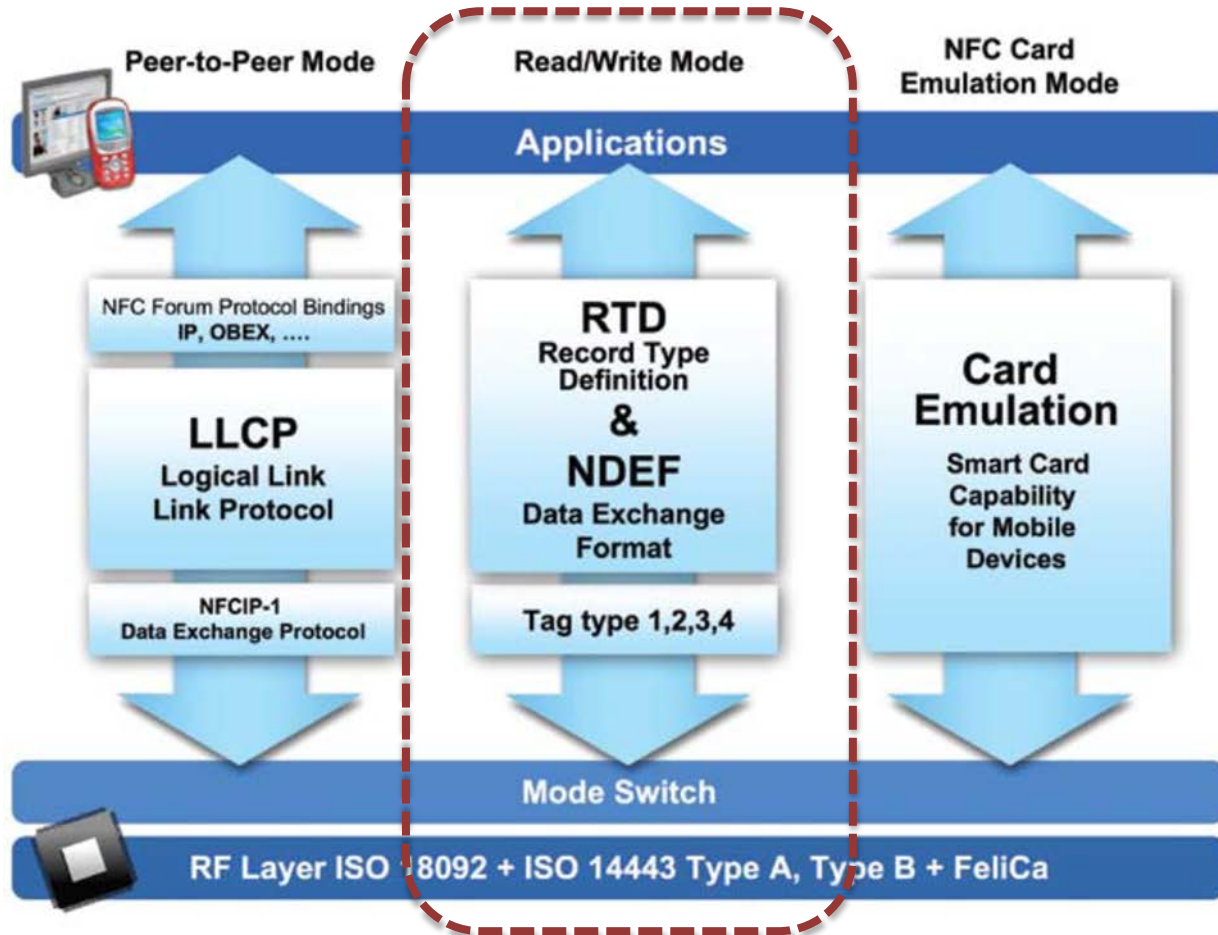
EMVCo/ISO/IEC14443, JIS X 6319-4/Felica



NFC Tag Basics

- **NFC tags are passive ICs used to communicate with active NFC devices**
 - Used within applications such as smart posters where small amounts of data (e.g., URLs) can be stored and transferred
- **NFC Forum has developed technical specifications to facilitate interoperability**
 - Define how (NDEF) messages are read from, and written to NFC tags
 - Well known Record Type Definitions (RTDs) include: NDEF, Text, URI, Smart Poster, and Signature

NFC Forum Architecture



NFC Forum Tag Types

	Type 1	Type 2	Type 3	Type 4
Sample of compatible products	Innovision Topaz	NXP Mifare L, UL-C Infineon SLE 66RxxP Kovio	Sony Felica	NXP DESFire NXP SmartMX-JOCP Calypso B
Memory Size	96 bytes 512 bytes	64 bytes 192 bytes 2048 bytes	1, 4, 9 Kbytes	2, 4, 8, 32 Kbytes
Standard	ISO14443A	ISO14443A	ISO 18092	ISO14443A and B
Speed	106 kbit/s	106 kbit/s	212 kbit/s	106 kbit/s and 424 kbit/s

An NFC Forum device is required to be able to read from, and write to, all tag types
 NFC tags vary in price depending on capacity and security capabilities

NFC Tag Security

Vulnerability	Attack	Mitigation	Note
Data modification e.g. smart poster	Replace tag with another i.e. phishing attack	NFC Forum Signature RTD - Data integrity	Adds no cost to the tag
Eavesdropping e.g. medical history	Listen from a distance	Encrypt the tag contents or password protected URL	Adds no cost to the tag - Tag could have an encryption engine (cost)
Data corruption/replacement e.g. any tag	Destroy the tag i.e. denial of service	Physical protection	Tag replacement can be detected using web analytics
Man in the middle e.g.. ticketing	Intercept and modify data without parties knowing	Secure challenge-response and/or encryption engine	Tag must have a crypto engine e.g. ticketing

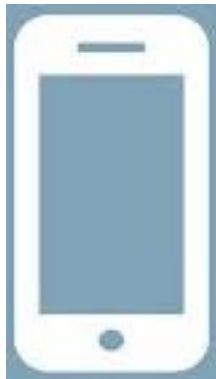
NFC Forum Signature RTD Technical Specification

➤ Similar to Web Browser Security

- Digital Certificates used to authenticate tags
- Tag authors digitally sign tags (i.e. NDEF records)

NFC root certificate

NDEF, Signature, Issuing Certificate



Active NFC-enabled device



NFC Tag



NFC root verifies signature on the tag's message



Smart Card
Alliance



NFC Tag Uses, Applications and Sourcing Considerations

- Joseph Tassone
- Executive Vice President Technology & Product Management
- Identive Group, Inc.



General NFC Tag Uses

- Linking physical & digital world
- Bringing ads/ content to life
- Engage with consumers
- Quick roll outs/ Re-use
- Diverse uses
- Simple but rich user experience: *social, video, sticky . . .*

Tag management bonus

Precise and trackable analytics:

- Are people engaging?
- What is working?
- Real time content tuning



Tag Application Areas



NFC & MOBILITY



**ACCESS &
TRANSPORTATION**



EVENT & LEISURE



GAMING



LOYALTY & PAYMENT



IDENTIFICATION

NFC & Mobility



NFC & MOBILITY

ACCESS &
TRANSPORT

EVENT &
LEISURE

GAMING

LOYALTY &
PAYMENT

IDENTIFICATION

NFC & Social use cases

Get easy & convenient access to:

- Discovery & Information sources
- Social Networks use – check in
- Bluetooth pairing, shopping lists
- Digital media content retrieval
- Marketing & brand development

Types

- All of NFC forum tag types
- Poster stickers
- Phone stickers
- Specialty by environment
- NFC tag content management platform



- *Transactions*
- *Discovery*
- *Exchange*



NFC & Mobility - Tag Examples

NFC & MOBILITY

ACCESS &
TRANSPORT

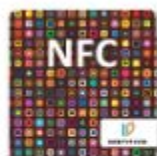
EVENT &
LEISURE

GAMING

LOYALTY &
PAYMENT

IDENTIFICATION

NFC Labels



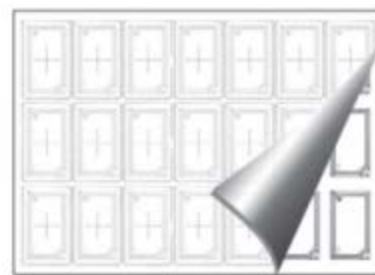
Magnetic metal shielded stickers

Shop-Window stickers

Social media stickers

and more ...

Customer Specific Tags



Tickets (paper, PET)
- singulated
- fanfold
- on roll

Smartcore™ the revolutionary card core

Special tags

and more ...

Access, Transportation & Leisure

Access, Transport & Leisure use cases

Fast & convenient use:

- Bus & Train tickets,
- Entrance to leisure parks
- Sports events, Ski tickets
- Trade Shows or group events



Types

- Inlays
- Standards for interstate and region
- Inlays, finished ticket types
- Higher data & security requirements



NFC & MOBILITY

ACCESS &
TRANSPORT

EVENT &
LEISURE

GAMING

LOYALTY &
PAYMENT

IDENTIFICATION

Gaming

NFC & MOBILITY

ACCESS & TRANSPORT

EVENT & LEISURE

GAMING

LOYALTY & PAYMENT

IDENTIFICATION

Gaming use cases

Fast & ease of use:

- New features for tech equipment, games or toys
- Game tokens
- Casino/ game chips
- Trade Show or group events



Types

- Inlays/ stickers for toys
- Molded tags
- Higher security requirements
- Brand & counterfeit protection



AVMB-USB

Loyalty & Payment

NFC & MOBILITY

ACCESS &
TRANSPORT

EVENT &
LEISURE

GAMING

LOYALTY &
PAYMENT

IDENTIFICATION

Loyalty & Payment use cases

Fast & ease of use:

- Personalized services
- Special offers, discounts
- Rewards programs
- Order menus
- Customer identity

Types

- Phone stickers
- Inlays/ stickers for posters/ counters
- Medium security requirements



cashless betalen
jouw manier van afrekenen



Identification



NFC & MOBILITY

ACCESS &
TRANSPORT

EVENT &
LEISURE

GAMING

LOYALTY &
PAYMENT

IDENTIFICATION

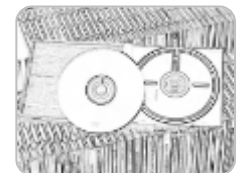
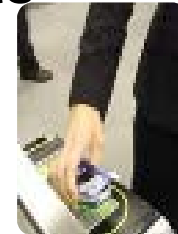
Authentication & Asset ID use cases

Inexpensive credentials:

- Physical or logical access
- Counterfeit protection
- Secure/ signed documents
- Asset tagging
- Process control

Types

- Inlays/ stickers /labels
- Higher security requirements
- RMA & service support





The Tag Value Chain Sources

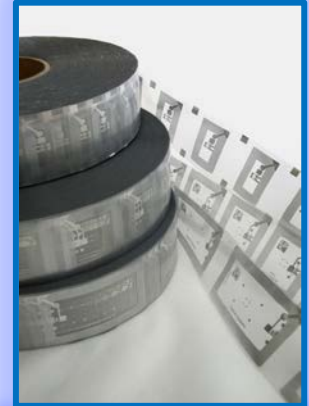
Smart Chips	<ul style="list-style-type: none"> •Chip type, Processing Options 	<ul style="list-style-type: none"> •NXP •Infineon •Sony 	<ul style="list-style-type: none"> •Broadcom •ST •Inside secure
Antennae	<ul style="list-style-type: none"> •RFID Expertise & Consulting •Standard and Custom Designs •Tag on Metal (tom® solutions) 	<ul style="list-style-type: none"> •Identive •UPM/Smartrac 	
Inlay Designs: Chip + Antenna	<ul style="list-style-type: none"> •Frequency Tuning Services 	<ul style="list-style-type: none"> •Identive •UPM/Smartrac 	
Embed Inlays in “Paper or Plastic”	<ul style="list-style-type: none"> •Tags, Cards, Fobs, Stickers •Shipped on a Roll, Fanfold, Singulated 	<ul style="list-style-type: none"> •Identive •UPM/Smartrac 	
Bulk Production	<ul style="list-style-type: none"> •High and Low Volume 	<ul style="list-style-type: none"> •Identive •UPM/Smartrac 	<ul style="list-style-type: none"> • Tagstand • Amazon
Bulk Printing Services	<ul style="list-style-type: none"> •Logos, text, enumeration, etc. 	<ul style="list-style-type: none"> •Identive •RapidNFC •TagAge 	<ul style="list-style-type: none"> • Tagstand
Bulk Encoding via NFC Readers	<ul style="list-style-type: none"> •Chip Initialization & Formatting •Chip Formatting •Label & Inlay Inkjet Printing (UID, serial number) 	<ul style="list-style-type: none"> •Identive •RapidNFC •TagAge 	
SDK's & Applications	<ul style="list-style-type: none"> •Cloud Based Tag Management Solutions •Content Management for Tags •Phone Apps 	<ul style="list-style-type: none"> •Identive •Proxama •NXP 	<ul style="list-style-type: none"> • Tagstand
2 way B2C Communication Deployments	<ul style="list-style-type: none"> •Pilots for Marketing Campaigns 	<ul style="list-style-type: none"> •Identive TagTrail •Proxama •BlueBite 	<ul style="list-style-type: none"> •Tagsquared •Connect Things

The Tag Costs - \$\$

<u>Item</u>	<u>Variables affecting Costs</u>	<u>Cost Range</u> <u>\$\$</u>
Inlays	<ul style="list-style-type: none"> • Chip type • Size • Material 	\$.25 - 1.00
Embedded Inlays in "Plastic or Paper"	<ul style="list-style-type: none"> • Materials • Handling form factor • Customization 	\$.35 – 1.25
Fully Finished & Printed	<ul style="list-style-type: none"> • Material / finish • Size • Printing quality 	.50 – 3.00
Finished w/ Personalization	<ul style="list-style-type: none"> • Chip format • Printing • Security required 	.75 – 5.00
NFC Readers, Writers, & Modules	<ul style="list-style-type: none"> • Reader form factors • Size • Versatility 	\$ 50 - 500

NFC Tag Costs

- **Factors affecting tag costs**
 - Chips used
 - Memory size
 - NFC Forum Type/ security req's
 - Materials employed – paper, plastics, polyester, etc.
 - Life & durability requirements
 - Specialty form factors
 - Other customization
- **Volumes & Source**





Smart Card
Alliance



Security for NFC Tag Applications

- Mike Zercher
- Senior Applications Engineer
- NXP Semiconductor

Why Do You Need Security

Security is used to protect data. The three objectives that you can do are :

- **Validate that data is yours.**
- **That the data has not been manipulated.**
- **That the data can not be read by someone else.**

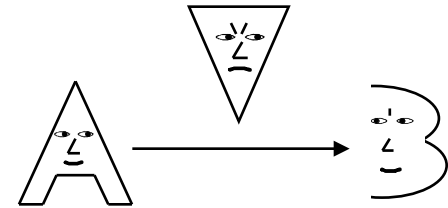
What Is Security

Security is based on cryptographic function to achieve one or more of the following

- **Authenticity**
- **Integrity**
- **Confidentiality**

What Do You Want to Achieve

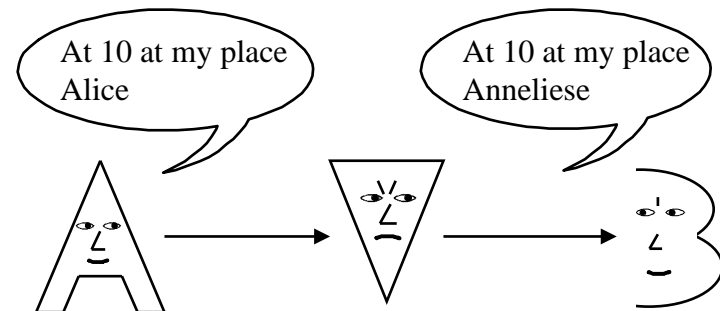
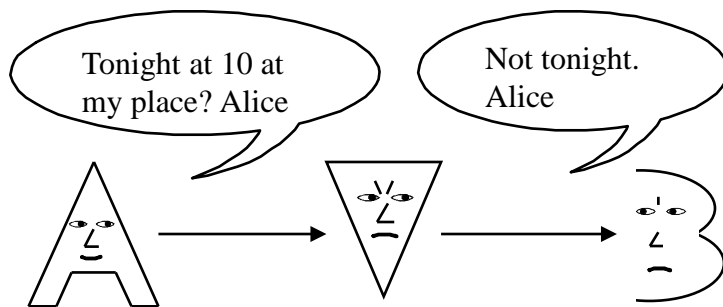
➤ Threat : Attacker's ability to read and change the data without detection



➤ Method : **Confidentiality**

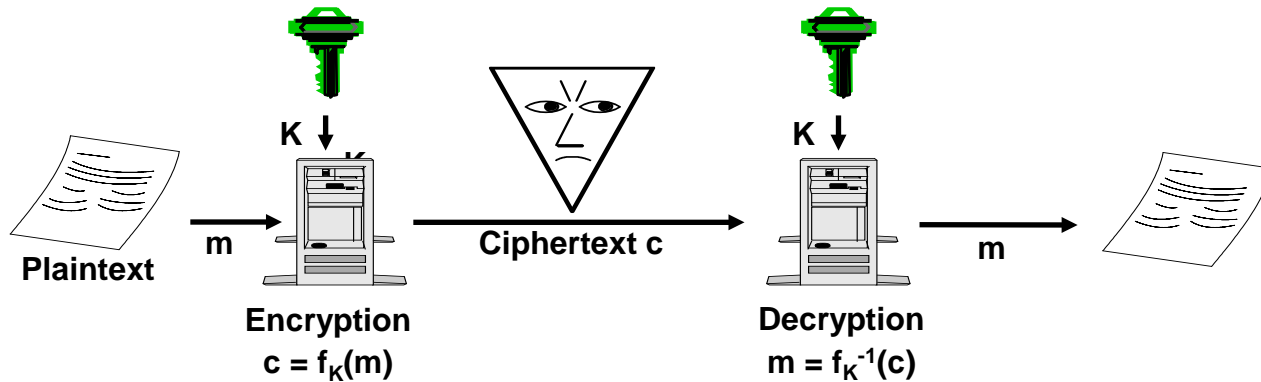
➤ Threat : Attacker's ability to change the data without detection

➤ Method: **Authenticity and Integrity**

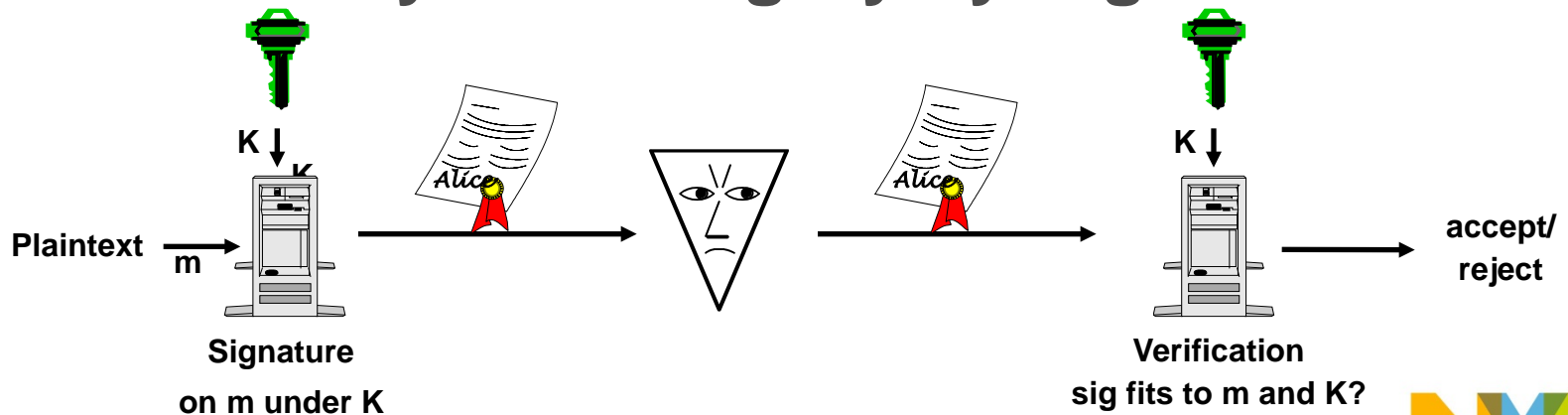


How to Achieve It

➤ Confidentiality by Encryption



➤ Authenticity and Integrity by Signatures



Employing Authenticity / Integrity to Tags

- **Developer may use NFC Forum Signature NDEF structure.**
 - Reference “NFC Forum Signature Record Type Definition Technical Specification version 1.0 “
- **Developer may define proprietary method of signature and associate the signature with data record.**
- **Signature NDEF record and corresponding data would be associated together**
 - Association by Reference
 - Association by Containment
 - Reference “NFC Forum NFC Record Type Definition

Employing Confidentiality

- **Only Payload will need to be encrypted**
- **Developer decides what encryption method to be used.**
- **Recommend only using standards based encryption (TDES, AES, RSA, etc).**
- **Both Developer and user needs to know what encryption and keys are used.**
- **Can be used in conjunction with Authenticity and Integrity methods.**

Takeaway on Security

Adding security to a tag requires analysis of cost versus benefits.

Protect only what you need; security adds a level of complication and time to the total transaction.

Newer tags have security functionality built into the chip but are not a part of the NFC tag specifications.



Smart Card
Alliance



Marketing and Market Directions

- Rob Zivney
- VP Marketing
- Identification Technology Partners





Smart Tags (& Stickers & Posters)

Research Stuff

- URL Links to Websites
- Product Data
- Dynamic Updates
 - Writable
 - Better than QR codes

Movies

- Launch Video Trailers

Privileges Wristbands

- Events, Theme Parks
- Spa & Fitness

Get Coupons etc

- Scan Tags
- Trade Show Promotions
- Storefront Promotions

Location Based Services

- Collect Data

Then Buy Stuff

- Via Mobile Wallet



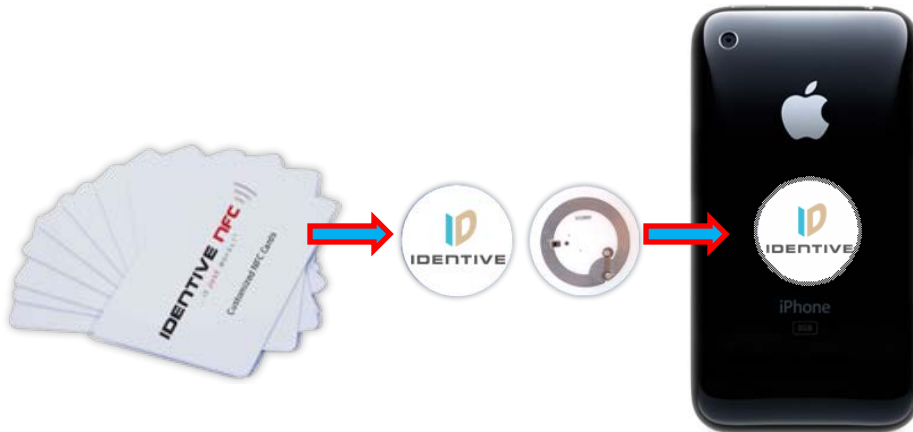
Stickers

The Essential NFC Enabler

- Posters, Products, Phones
- Evolution of Smart Card Form Factor
 - Same Service Provider Model
- Role Reversals
 - Easy NFC Migration

Phone Enablement

- Passive
 - No Connection to OS
 - No Dynamic App Management
 - For Payment & Loyalty
 - For Physical & Logical Access
- Good Migrations
 - “Tag in a Box” (with a new NFC Phone)



NFC TAG Technology

Benefits

- 2 Way Communications
- Low Friction Setup
 - No Discovery - No pairing
 - Can Bootstrap Bluetooth & WiFi
- Automatic! No Need to Launch App
 - Instant Gratification...It Just Works!
- Touch Sharing
 - Content, Web Page, Video, Apps
- Identify Documents
- Supports Encryption (MIFARE DESFire)
 - App Can Implement Encryption
- NFC is Off When Phone Screen is Off
 - No Butt Sniffing
- No Link Level Encryption
 - App Must Implement Encryption
- No API for Card Emulation Support in Gingerbread (Android)
 - Available in ICS

Standards

- Passive (Unpowered) Tags & Stickers
- Includes ISO/IEC 14443, ISO/IEC 18092
- Short Range RFID Technology (1-4cm)
 - 13.56MHz
- Low Speeds (106-414 kbps)
- Data Structures < 1KB (type 4 tag, 2KB)
- Standards Defined by NFC Forum
 - NDEF is Standardized Data Format
 - Supports Encryption (MIFARE DESFire)
 - More Private than 125Khz Prox
- Various NDEF record types for specific cases:
 - Smart posters
 - URLs, SMSs, or phone numbers on tag
 - Read now, process later
 - Trigger apps
 - Launch a browser - View a website
 - Send SMS to a service to receive a ring tone
 - URI's
 - Digital Signatures
 - Text
 - vCard

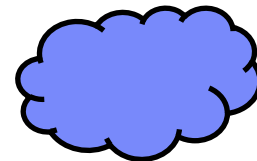


Tags – What about the SE?

- **Tags Work with Phone in Reader/Writer Mode**
- **Reader/Writer Mode Doesn't Use the SE!!!**
 - SE Used with Card Emulation Mode
 - Not Relevant for Smart Posters & Tags
- **Tags are Passive to Phones in Reader/Writer Mode**
- **Smart Tag Apps Typically Don't Need a Secure Area in Mobile Phones**
 - Just Reading (or Writing) Non-Secure Data on a Tag
- **Tag Apps & Use Cases Can Lead Market Growth**

Tagging - The User Experience!

- **Events**
- **Locations**
- **Discovery**
- **Experience**
- **Memories**
 - Relive the Experience
 - Social Media Exchange - Sharing
- **If We Connect the Event to Business Logic...**
- **New Service Opportunities**
 - SaaS – Software as a Service
 - Cloud Apps

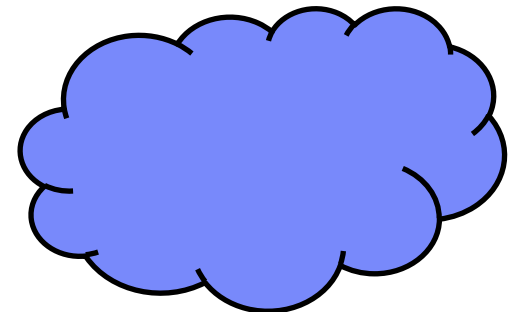


SaaS Business Model Concepts

Initiation Fee
Per Tag Managed
Tag Location
Per User
Per Click
Per Time Period
Revenue Share



Consumer Focus
Cloud Enabled



Tag Management - Analytics

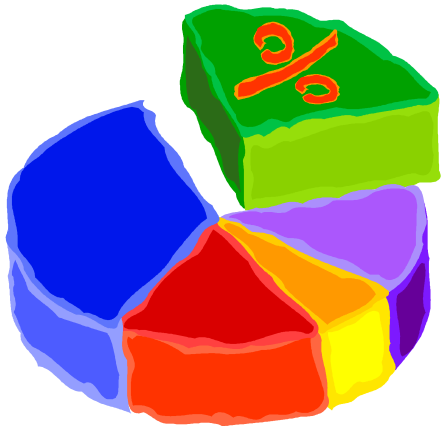
Trackable

- Precise

Are People Engaging?

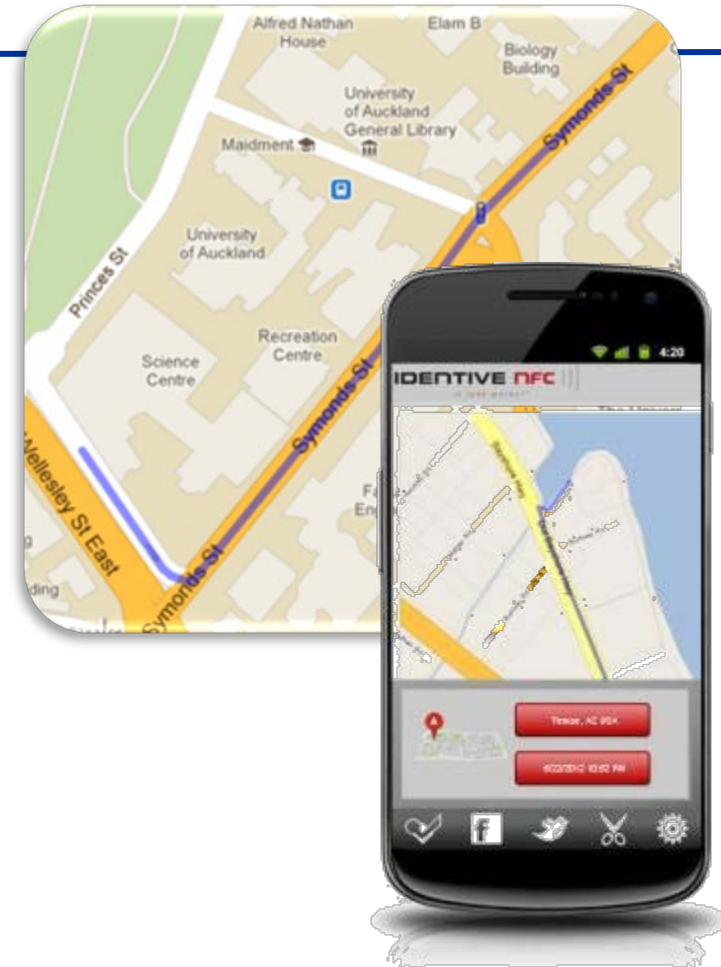
What is Working?

Real Time Content Tuning



NFC Tag Management Solution

- **Offers “Me-Based” Services**
- **Make It Personal**
 - Based on User Profile & Further Parameters
- **Dynamic Tag Content Engine**
 - Manage Content per Each Tap
- **“Me-Based” Content:**
 - What I Want
 - When I Want it
 - Micro Opt-in Option



Many Cloud Based NFC Tag Management Applications!

- Physical access
- Payment
- Loyalty & reward
- Advertisement
- Ticketing
- Promotions
- Membership Management
- Directions
- Asset tracking





Smart Card
Alliance



Questions & Answers





Mobile & NFC Security Webinar Series

- **Mobile/NFC Security Fundamentals : NFC Application Use Cases – Security Perspectives**
 - May 9, 2013, 1pm ET/10am PT
 - **Speakers:** Rene Bastien, SecureKey Technologies; Jonathan Main, NFC Forum/MasterCard; Steve Rogers, IQ Devices; Tony Sabetti, Isis; Randy Vanderhoof, Smart Card Alliance



NFC Solutions Summit 2013



NFC SOLUTIONS SUMMIT 2013

SMART SECURE MOBILE PAYMENTS AND NON-FINANCIAL NFC APPS

May 15-16 | Hyatt Regency San Francisco Airport | Burlingame, California





Smart Card Alliance



- Tony Rosati, trosati@rim.com
- Joe Tassone, jtassone@identive-group.com
- Randy Vanderhoof, rvanderhoof@smartcardalliance.org
- Mike Zercher, mike.zercher@nxp.com
- Rob Zivney, rzivney@idtp.com

Smart Card Alliance

191 Clarksville Rd. · Princeton Junction, NJ 08550 · (800) 556-6828

www.smartcardalliance.org

